UNIVERSIDADE NOVA DE LISBOA

MESTRADO EM DIREITO E SEGURANÇA

Dissertação

A Aplicação do Uso da Força no Ciberespaço

Mestrando: **Ricardo Alexandre Rodrigues Caiado**

Orientador: **Professor Doutor José Fontes**

Lisboa, 31 de julho de 2020

Declaração de compromisso Antiplágio

Eu, Ricardo Alexandre Rodrigues Caiado, declaro por minha honra que o documento intitulado "A Aplicação do Uso da Força no Ciberespaço", corresponde ao resultado da investigação por mim desenvolvida, enquanto mestrando do Mestrado em Direito e Segurança e que se trata de um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.
Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Lisboa, 31 de julho de 2020

Ricardo Alexandre Rodrigues Caiado

À CLÁUDIA

Agradecimentos

A execução de uma dissertação de Mestrado não é uma obra que se possa realizar de forma isolada, sem a colaboração de pessoas que, quer pelas qualidades técnicas que possuem ou pela relação afetiva que têm com o autor, dão preciosas indicações e um apoio incomensurável à concretização da mesma.

Ao longo dos vários meses em que realizei este trabalho de pesquisa fui colhendo diversos apoios ao nível pessoal bem como da instituição na qual produzi este trabalho de investigação, aos quais é, agora, chegado o momento de lembrar e agradecer.

O meu primeiro agradecimento pessoal vai para o meu orientador, o Professor Doutor José Fontes pelo apoio incondicional prestado e pela permanente disponibilidade, bem como pelo interesse demonstrados na condução deste trabalho, pelos esclarecimentos e pertinentes sugestões.

Em segundo lugar, agradecer a todos os professores da Universidade Nova de Lisboa que contribuíram para o meu desenvolvimento pessoal e inteletual, bem como possibilitaram mais uma etapa nesta caminhada pelo saber, um sentido bem hajam.

De igual modo, quero igualmente expressar o meu agradecimento a todos os meus amigos e colegas, que contribuíram direta ou indiretamente, com a sua crítica, discussão e estímulo para a realização deste trabalho.

Por fim, e não menos importante, à minha esposa Cláudia pelo constante apoio, compreensão e estímulo que me foi dando ao longo de mais esta caminhada na área do saber, a qual indubitavelmente se traduziu em muitas horas em que se viu privada da minha companhia, disponibilidade, atenção e carinho.

A todos, os meus sinceros agradecimentos

"Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas…"

Sun Tzu

Resumo

O presente trabalho foi elaborado no âmbito do Mestrado em Direito e Segurança da Faculdade de Direito da Universidade Nova de Lisboa, e teve como desiderato procurar responder à seguinte questão: "Quais são os limites legais de aplicação do uso da força no ciberespaço?"

Para tal, iremos abordar a segurança no ciberespaço, passando ainda pela análise sumária aos ciberataques à Estónia em 2007, e alguns considerandos relativos à cibercriminalidade, problemática que cada dia mais faz parte do nosso quotidiano. De igual modo, e devido à sua atualidade e pertinência, analisaremos os fenómenos do terrorismo e do ciberterrorismo.

Após este enquadramento, iremos delimitar o uso da força, bem como serão explicitados alguns conceitos importantes para percebermos como funciona o princípio geral de proibição do uso da força, tais como, o conceito de agressão, e o que significam os conceitos de "*jus ad bellum*" e de "*jus in bello*", bem como as suas diferenças. Abordaremos também a exceção à proibição do uso da força, que se traduz na legítima defesa, nos termos do art.º 51.º da Carta das Nações Unidas e procuraremos explicitar qual o contributo do Manual de Tallinn, enquanto enquadrador de boas práticas de Direito Internacional, as quais acabarão por condicionar a definição de novos conceitos jurídicos e procedimentos de resposta aos ciberataques.

Para terminar, será objeto de análise a problemática do uso da força no ciberespaço, a qual será antecedida por um breve enquadramento relativo à ciberdefesa, bem como uma análise aos princípios da guerra clássicos, no sentido de perceber como é feito o uso da força numa perspetiva mais tradicional de um conflito armado.

O objetivo final desta caminhada será perceber de facto quais são os limites legais de aplicação do uso da força, através dos vários normativos legais e de boas práticas que são abordados neste estudo. Contudo, não poderíamos deixar de aproveitar a oportunidade para também deixar uma margem de reflexão para a necessidade de adequação dos conceitos da Arte da Guerra mais tradicional para uma Guerra que ocorre no Ciberespaço, onde o conceito de fronteira é de difícil definição, bem como a forma como cada Estado se movimenta neste tabuleiro de xadrez virtual assume contornos completamente distintos.

Palavras-Chave: Uso da Força, Ciberespaço, Cibersegurança, Ciberataques, Estónia, Cibercriminalidade.

Abstract

The present work was elaborated in the scope of the Master in Law and Security of the Faculty of Law of the New University of Lisbon, and had as aim to answer the following question: "What are the legal limits of application of the use of force in Cyberspace?"

To this end, we will address security in cyberspace, including the summary analysis of cyber attacks to Estonia in 2007, and some considerations regarding cybercrime, a problem that is increasingly part of our daily lives. Likewise, and due to its relevance and relevance, we will analyze the phenomena of terrorism and cyberterrorism.

After this framework, we will delimit the use of force, as well as explain some important concepts to understand how the general principle of prohibition of the use of force works, such as the concept of aggression, and what the concepts of "*jus ad bellum*" and "*jus in bello*", as well as their differences. We will also address the exception to the prohibition on the use of force, which translates into self-defense, under the terms of article 51 of the Charter of the United Nations and we will try to explain what the Tallinn Manual contributed, as a framework for good law practices International, which will ultimately condition the definition of new legal concepts and procedures for responding to cyber attacks.

Finally, the issue of the use of force in cyberspace will be the object of analysis, which will be preceded by a brief framework related to cyber defense, as well as an analysis of classical war principles, in order to understand how force is used in a more traditional perspective of armed conflict.

The ultimate goal of this journey will be to understand the legal limits of the use of force through the various legal norms and good practices that are addressed in this study. However, we could not take the opportunity to also leave room for reflection on the need to adapt the concepts of the more traditional Art of War to a War that occurs in Cyberspace, where the concept of boundary is difficult to define, as well as the way each state moves in this virtual chessboard assumes completely different contours.

Keywords: Use of Force, Cyberspace, Cybersecurity, Cyber attacks, Estonia, Cybercrime.

Lista de abreviaturas, siglas e acrónimos

ADM	Armas de Destruição Maciça
AP	Administração Pública
AR	Assembleia da República
AREAII	Artigos sobre Responsabilidade dos Estados por Atos Internacionais Ilícitos
CBC	Convenção de Budapeste sobre Cibercrime
CCDCOE	Centro de Excelência em Defesa Cibernética Cooperativa da OTAN
CE	Comissão Europeia
CEDH	Convenção Europeia dos Direitos do Homem
CEDN	Conceito Estratégico de Defesa Nacional
CNA	*Computer Network Attack*
CNCS	Centro Nacional de Cibersegurança
CND	*Computer Network Defense*
CNE	*Computer Network Exploitation*
CNO	*Computer Network Operations*
CNU	Carta das Nações Unidas
CP	Código Penal
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
CS	Conselho de Segurança
CSIRT	*Computer Security Incident Response Team*
CSSC	Conselho Superior de Segurança do Ciberespaço
CVDTE	Convenção de Viena sobre o Direito dos Tratados entre Estados
DDoS	*Distributed Denial of Service*
DIH	Direito Internacional Humanitário
DIP	Direito Internacional Público
DLG's	Direitos, Liberdades e Garantias
DN	Defesa Nacional
DoS	*Denial of Service*
DUDH	Declaração Universal dos Direitos do Homem
EC3	Centro Europeu de Cibercrime
EDA	Agência Europeia de Defesa
EM	Estados Membros

EMGFA	Estado-Maior-General das Forças Armadas
ENCS	Estratégia Nacional de Cibersegurança
ENS	Estratégia Nacional de Segurança
ENSC	Estratégia Nacional de Segurança do Ciberespaço
ENISA	Agência da União Europeia para a Segurança das Redes e da Informação
ESE	Estratégia de Segurança Europeia
ESIUE	Estratégia de Segurança Interna da União Europeia
EUMS	*European Military Staff*
FA	Forças Armadas
FS	Forças de Segurança
FSS	Forças e Serviços de Segurança
GGE	*Group of Governmental Experts*
GNR	Guarda Nacional Republicana
IC	Infraestruturas Críticas
ICT	*Information and Communications Tecnology*
INFOSEC	*Information Security*
IoE	*Internet of Everything*
IoT	*Internet of Things*
ITU	*International Telecommunication Union*
LC	Lei do Cibercrime
LSI	Lei de Segurança Interna
MP	Ministério Público
NCIRC	NATO *Computer Incident Response*
NIST	*National Institute for Standards and Technology*
NU	Nações Unidas
OCDE	Organização para a Cooperação e Desenvolvimento Económico
OI	Organização Internacional
ONU	Organização das Nações Unidas
OPC	Órgãos de Polícia Criminal
OSCOT	Observatório de Segurança, Criminalidade Organizada e Terrorismo
OTAN	Organização do Tratado do Atlântico Norte
PCSD	Política Comum de Segurança e Defesa
PE	Parlamento Europeu

PR	Presidente da República
RCM	Resolução do Conselho de Ministros
SI	Segurança Interna
SII	Sistemas de Informação
SIC	Sistemas de Informação e Comunicação
SSI	Sistema de Segurança Interna
TFUE	Tratado sobre o Funcionamento da UE
TIC	Tecnologias de Informação e Comunicação
TIJ	Tribunal Internacional de Justiça
TPI	Tribunal Penal Internacional
UE	União Europeia

Índice

Índice de Tabelas

Introdução

O presente trabalho, intitulado "*A Aplicação do Uso da Força no Ciberespaço*", elaborado no âmbito do Mestrado em Direito e Segurança da Faculdade de Direito da Universidade Nova de Lisboa, tem como principal objetivo fazer uma breve análise dos fenómenos ligados ao mundo do ciberespaço, numa perspetiva de constante mutação e adaptação às novas tipologias de guerra e de crime ou, pelo menos, da mudança do seu *modus operandi*, com as consequentes alterações na Estratégia que cada Estado leva a cabo.

O atual trabalho assume-se como um passo importante na concretização do desiderato referido previamente, possibilitando aos alunos o conhecimento de diversos conceitos relacionados com a área em estudo nas diversas unidades curriculares deste Mestrado.

A metodologia utilizada neste trabalho assenta na sustentação teórica baseada numa pesquisa documental de diversa bibliografia, de forma a recolher o maior número de informações relativamente à temática a que nos propomos tratar. De igual modo, iremos usar a abordagem positivista e com a breve análise de um estudo de caso internacional, considerando a sua pertinência para o tema em análise.

Este trabalho partiu da questão central: Quais são os limites legais de aplicação do uso da força no ciberespaço? Da questão central foram elaboradas três questões derivadas, a saber: QD1 De que forma se aplica o uso da força no ciberespaço? QD2 De que forma o Direito Internacional e as boas práticas condicionam o uso da força no ciberespaço? QD3 Quais as repercussões que o uso da força, à luz do Direito Internacional, condiciona a aplicação do uso da força no ciberespaço?

Após a definição da já elencada questão central enunciámos as seguintes hipóteses:

H1: As ciberameaças condicionam o recurso ao uso da força à luz do Direito Internacional, dificultando a sua tipificação e aplicação.

H2: O uso da força no ciberespaço é feito com base na Carta das Nações Unidas.

H3: A legítima defesa pode ser feita por qualquer Estado que seja atacado no âmbito da Guerra Cibernética.

H4: O Manual de Tallinn condiciona a Estratégia de Implementação de um plano de ação para o combate ao cibercrime.

1. Enquadramento Geral

1.1. A Segurança no Ciberespaço

1.1.1. Breve enquadramento

> "A estruturação em rede das sociedades mais desenvolvidas e a própria construção do ciberespaço constituem caraterísticas fundamentais da conjuntura estratégica do século XXI. Neste contexto, pensar o mundo em que vivemos passa por perspetivar uma sociedade em rede, em que a interação entre os homens deixa de ser influenciada por barreiras geográficas e passa a ser condicionada pela disponibilidade e pelo tempo de acesso aos recursos de informação."[1]

Antes de abordarmos a segurança no ciberespaço[2], vamos fazer um pequeno enquadramento no que à internet diz respeito, de forma a melhor compreender a sua importância e o porquê de atualmente já não ser quase possível viver sem o recurso à mesma.

O aparecimento da internet surgiu numa altura coincidente com o início da Guerra Fria, tendo os primeiros computadores aparecido na década de 1950. O seu surgimento fica ligado à necessidade identificada pelos EUA de interligar máquinas de uma "forma eficiente, descentralizada e resiliente, (…) no caso de um ataque nuclear"[3], tendo desta forma nascido o projeto *Advanced Research Projects Agency Network* (ARPANET), do Departamento de Defesa dos EUA, o qual se considera como o antepassado da atual internet, enquanto "método global de comunicação por excelência"[4].

Assim, podemos afirmar que a "internet revolucionou o mundo das comunicações e das relações pessoais de uma maneira sem precedentes", a qual se afigura como uma "ferramenta mundial de radiodifusão, de disseminação de informação, um meio para colaboração e interação entre indivíduos e seus computadores, independentemente de sua localização geográfica".[5]

---

[1] INSTITUTO DA DEFESA NACIONAL – **Estratégia da Informação e Segurança no Ciberespaço.** N.º 12. Lisboa: IDN, 2013. ISBN: 978-972-27-2272-8. p. 8.

[2] Ciberespaço é um "termo que aparece originalmente num livro de ficção científica em 1984, Neuromancer, de William Gibson", sendo definido pela Porto Editora como o "espaço virtual constituído por informação que circula nas redes de computadores e telecomunicações". "A *International Standard Organization* (ISO) vai mais longe, definindo-o como "um ambiento complexo que resulta da interação das pessoas, *software* e serviços na internet, suportado pela distribuição mundial de equipamentos e redes de informação física e tecnologias de informação." ANTUNES, David – **O Hacktivismo e as FA.** Lisboa: Instituto de Estudos Superiores Militares, 2013. Trabalho de Investigação Individual do CEMC – 2012/13. p. 5. De igual modo, refira-se que o "ciberespaço é muito mais amplo do que a internet, pois interliga também outras redes de computadores, por vezes separadas da Internet, como são as redes transacionais de fluxos monetários, do mercado acionista, cartões de crédito e sistemas de controlo de todo o tipo. As sociedades ocidentais têm alimentado uma adição crescente ao, e no ciberespaço." ANTUNES – ***Op cit.*** p. 7.

[3] *Ibidem*.

[4] *Ibidem*.

[5] FERNANDES, Filipe – **A Cibersegurança e as Estruturas Críticas: A GNR. Ciberguarda, o Futuro.** Lisboa: Academia Militar, 2013. Dissertação de Mestrado. p. 13.

A internet pode assim ser considerada como "o mais significativo desenvolvimento na história das comunicações, uma vez que liga indivíduos, instituições e tudo o que está entre eles, de uma forma sem precedentes"[6], facto que consubstanciou um aumento exponencial da tecnologia e o desenvolvimento do ciberespaço. Nesta sequência, o termo ciberespaço passou "a integrar o léxico comum, sendo vulgarmente utilizado para descrever o mundo virtual que os utilizadores da Internet visitam quando estão *online*, acedendo aos mais diversos conteúdos[7] (…) que a rede mundial de computadores disponibiliza"[8].

Com efeito, a importância que a internet tem atualmente na nossa sociedade tem conduzido a um maior envolvimento dos governos nesta problemática da rede.[9]

O desenvolvimento da internet teve uma grande alavanca com o surgimento da banda larga e, de igual modo, com a facilidade e reduzidos custos de aquisição de computadores pessoais[10].

A referida evolução conduziu a um novo paradigma de sociedade, o qual se consubstancia numa sociedade global[11], sem fronteiras, e permanentemente interligada entre todos, bem como assume um papel vital na política[12].

---

[6] NATÁRIO, Rui – **O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço.** [Em Linha]. Lisboa: Revista Militar, 2016. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.revistamilitar.pt/art.º.php?art_id=854. p. 7.

[7] Em 1997, o Ministério da Ciência e da Tecnologia definiu "a palavra conteúdo", referindo, "no seu Livro Verde para a Sociedade da Informação", que "no contexto emergente da Sociedade da Informação, o termo "conteúdo" parece englobar todo e qualquer segmento de informação propriamente dito, isto é, tudo aquilo que fica quando excluímos os sistemas de *hardware* e *software* que permitem a sua consulta e exploração". CASIMIRO, Sofia – **A Responsabilidade Civil pelo Conteúdo da Informação Transmitida pela Internet.** Coimbra: Almedina. 2000. p. 15. Cfr. COSTA, João – **A responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na Internet - Em especial da responsabilidade pelos conteúdos gerados por utilizadores.** Porto: Faculdade de Direito da Universidade de Direito, 2011. Dissertação de Mestrado. p. 19.

[8] NATÁRIO – ***Op cit.*** p. 2.

[9] "Se alguns governos se preocupam sobre o impacto económico e social da rede, do seu uso como instrumento de desenvolvimento e democraticidade, outros procuram controlar a rede para evitar que esta seja usada para fins políticos contrários aos seus interesses. É neste mundo de enorme diversidade que o problema da governação da internet se move, procurando seguir abordagens inovadoras e que garantam um crescente uso da rede com segurança, estabilidade e abrangência universal."VEIGA, Pedro; DIAS, Marta – **A Internet e as novas dimensões legais.** [Em Linha]. Lisboa: Universidade Autónoma de Lisboa, 2012. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: http://janusonline.pt/popups2011_2012/2011_2012_1_5.pdf.

[10] "Em consequência, houve um aumento desmesurado de informação, com um custo de acesso insignificante e com uma capacidade de alcance virtual mundial, causando novos problemas como os da sobrecarga da informação e da difusão do poder, para os quais nos alerta Nye, quando afirma que a disseminação da informação significa que o poder será distribuído de forma mais vasta e as redes informais vão minar o monopólio da burocracia tradicional". DOMINGUES, Elisabete **– Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo.** Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna, 2015. Dissertação de Mestrado. p. 8.

[11] A internet provocou uma revolução na história da humanidade, assumindo assim "uma grande relevância, quer através do setor económico criado pelo comércio eletrónico, quer através da influência cultural e educativa que ela exerce, abrindo cada vez mais possibilidades aos seus utilizadores". Todavia, não poderemos esquecer que a "internet é igualmente suscetível de ser utilizada para fins ilegais ou lesivos, podendo assim desencadearem-se hipóteses de responsabilidade civil. Em termos gerais, podemos apontar as seguintes situa-

Nesta perspetiva, registe-se que o "avanço da tecnologia e a constante vontade de acompanhar os sucessivos progressos informáticos despertaram a importância de proteger cada cidadão[13] dos riscos inerentes a este universo cibernético"[14].

A referida proteção de cada cidadão, implica a defesa dos seus direitos fundamentais, nos quais se envolve "a proteção da privacidade, preocupação constitucional quando se prevê que todos têm direito à reserva da intimidade da vida privada e à sua imagem"[15].

A evolução tecnológica e a globalização vieram potenciar as ameaças à privacidade dos cidadãos, seja na interação entre as pessoas ou entre as mesmas e o Estado. Deste modo, a "partilha de informações pelos próprios utilizadores de internet e o seu armazenamento em *cloud*[16]colocam em risco o controlo desses dados pelos próprios titulares"[17].

Este paradigma conduz à necessidade de os Estados terem a capacidade de mitigar "o problema das ameaças à segurança dos cidadãos, protegendo-os inclusive da criminalidade organizada, mesmo a transnacional, sem deixar ao mesmo tempo de prover a que os dados pessoais não sejam utilizados indevidamente, nem a privacidade das pessoas injustificadamente atingida"[18].

ções juridicamente tuteladas para as quais a utilização da internet poderia constituir fonte potencial de riscos", entre outras: "a segurança da própria informação eletrónica, através do ataque por *hackers* aos *sites* nela disponibilizados; e a tutela da vida privada, como no caso da transferência não autorizada de dados pessoais." LEITÃO, Luís – **A Responsabilidade Civil na Internet.** Conferência realizada na Associação Empresarial de Portugal, em 16 de novembro de 2000. [Consult. 21 Set. 2018]. Disponível em WWW:<URL: http://www.oa.pt/upl/%7B034a6b68-6f5e-4eb9-b57b-06a413387077%7D.pdf. p. 172-173.

[12] VEIGA – ***Op cit.***

[13] "Os direitos fundamentais consubstanciam o reflexo da sociedade onde o Homem convive em cada época, resultantes das necessidades historicamente impostas", assumindo tais direitos uma "função de escudo protetor determinados em cada contexto sócio-político". Cfr. FERREIRA, Pedro – **A Proteção de Dados Pessoais na Sociedade de Comunicação - Dados de Tráfego, Dados de Localização e Testemunhos de Conexão.** Lisboa: O Espírito das Leis, 2006. p. 71. e OLIVEIRA, Margarida – **Proteção de Dados Pessoais nas Comunicações Eletrónicas: O papel da CNPD e da ANACOM.** Lisboa: Universidade Católica Portuguesa, Faculdade de Direito, 2015. Dissertação de Mestrado. p. 15.

[14] OLIVEIRA – ***Op cit.*** p. 5.

[15] VAZ, Ana – Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais. In **Nação e Defesa.** N.º 117. 3.ª Série. Lisboa: Instituto de Defesa Nacional, 2007. p. 37.

[16] Armazenamento em servidores à distância, designadamente, em outros países, que permitem que a informação esteja acessível em qualquer parte do mundo, sem que a pessoa tenha que levar dispositivos móveis de armazenamento consigo.

[17] DUARTE, Vânia – **Protecção de dados pessoais na internet: o caso do "direito a ser esquecido".** Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2014. Dissertação de Mestrado. p. 6.

[18] "A segurança e a privacidade são assim valores que devem estar associados à utilização dos sistemas de informação uma vez que é nestes sistemas que se baseiam as atividades dos Estados, das instituições, das empresas e dos cidadãos." VAZ – ***Op cit.*** p. 38.

Deste modo, os "sistemas de segurança da informação devem também ter em conta as ameaças[19] que hoje se colocam às liberdades individuais, à proteção dos dados pessoais e consequentemente à privacidade"[20].

Considerando a atual sociedade em rede, as ameaças são essencialmente direcionadas aos "sistemas de informação[21] organizacionais, independentemente do tipo de organização, da dimensão, da natureza (pública ou privada) e dos recursos de tecnologias de informação e comunicação (TIC) existentes"[22].

A fim de mitigar estas ameaças, verifica-se a necessidade da implementação de "uma *framework* de segurança[23], para garantir fundamentalmente a segurança dos recursos de informação, integrando diferentes visões: a da comunidade científica (modelo conceptual), a perceção dos decisores (modelo comportamental) e o modelo tecnológico de suporte aos processos de negócio"[24].

Neste contexto, assume particular importância a segurança na internet. Deste modo, a correta "utilização dos serviços associados à internet (…) contribui para a prevenção das ameaças já referidas, garantindo para uma maior resiliência dos sistemas de informação e para a continuidade dos "processos funcionais" (…), diminuindo os riscos associados à "segurança de informação", assegurando a confidencialidade[25], a disponibilidade[26], a integridade[27] e a autenticidade[28] dos dados que residem, circulam e que são processados"[29] nos mais variados sistemas de informação.

---

[19] "A evolução tecnológica contribui para que as organizações automatizem seus serviços, em direção a maior eficiência e eficácia. Mas há uma contrapartida do processo, que demanda cuidados frente às ameaças a que se tornam expostos os sistemas de informação e comunicação, especialmente quando conectados à rede mundial de computadores." FERNANDES, Jorge – **Gestão da segurança da informação e comunicações.** Vol. 1. Brasília: Universidade de Brasília, Faculdade de Ciência da Informação, 2010. Série Segurança da Informação. ISBN 978-9949-9211-2-6. p. 27.

[20] "A informação é um recurso que tem valor essencial para as organizações, incluindo-se nesta aceção os Estados: é um valor decisivo e fundamental nos dias em que vivemos e assume um aspeto relevante na segurança e defesa das nações. Qualquer interrupção de serviço público, utilização indevida de informação classificada ou destruição de dados de cariz importante pode pôr em causa a confiança dos cidadãos e os interesses – e até a própria soberania – dos Estados." VAZ – ***Op cit.*** p. 39.

[21] Os sistemas de informação são um fator determinante para a competitividade das organizações, constituindo uma ferramenta que estimula a sua produtividade, imprescindível ao processo de tomada de decisão aos vários níveis de gestão.

[22] MARTINS, José – **Framework de Segurança de um Sistema de Informação.** Guimarães: Universidade do Minho, 2008. Dissertação de Mestrado. p. 3.

[23] Cfr. MARTINS – ***Op cit.*** p. 73.

[24] "Para proteger uma organização das ameaças à segurança da sua informação ou da que está sob a sua responsabilidade, deve a organização possuir uma política de segurança, sendo necessária simultaneamente uma identificação e avaliação de riscos." MARTINS – ***Op cit.*** p. 3.

[25] Propriedade que garante que a informação não está disponível ou é revelada a indivíduos não autorizados, entidades ou processos.

[26] Propriedade que garante que a informação seja acessível e utilizável por uma entidade autorizada.

[27] Propriedade que garante que um dado não seja modificado sem autorização.

Como tal, na Europa "assiste-se a uma crescente atenção para os problemas na área da governação[30] da internet"[31], pelo que existem alguns aspetos legais da internet a ter conta, tais como: "a proteção dos dados pessoais; a defesa dos direitos de propriedade intelectual e direitos conexos; a luta contra a cibercriminalidade; a proteção dos menores, a quem é reconhecida especial debilidade no âmbito da utilização diária dos recursos da rede, em particular, das redes sociais; os direitos dos consumidores em geral; os eventuais constrangimentos no acesso comercial aos serviços de internet e a respetiva regulação pelas autoridades competentes em cada país"[32].

As já referidas ameaças presentes na internet, bem como a exponencial conexão de milhões de redes informáticas, sistemas de informação, pessoas e objetos, levam à propensão de todo o "género de práticas de índole delituosa, subversiva e beligerante, em que se enquadra desde a simples delinquência juvenil até ao hactivismo, o cibercrime, o crime organizado, a ciberespionagem, o ciberterrorismo e a ciberguerra"[33].

Assim, as "ameaças ao ciberespaço, ou à realidade que o mesmo engloba, podem ser várias e estão divididas na literatura essencialmente em cinco dimensões: o cibercrime, o hacktivismo, o ciberterrorismo, a ciberespionagem e a ciberguerra"[34].

A era de transformação digital em que vivemos serviu de mote à "emergência do *crime as a service*", uma vez que, para além do hacktivismo, existe atualmente uma espécie de catálogo onde crimes digitais são oferecidos a troco de dinheiro.[35]

---

[28] Propriedade que nos diz que uma entidade é aquilo que realmente afirma ser.

[29] **Portal de Cibersegurança da GNR** [Em Linha]. [Consult. 05 Out. 2019]. Disponível em WWW:<URL: http://portalciber.gnr.local/wordpress/index.php/2015/12/28/seguranca-na-internet/.

[30] "No âmbito da gestão da informação, a informação tem-se tornado, cada vez mais, um importante recurso na vida das pessoas e, particularmente, nas atividades operacionais e estratégicas das instituições e organizações, com o rápido desenvolvimento das TIC, observado na Era Digital. Nesse cenário, este recurso passa a ser capaz de marcar a diferença entre o sucesso e o insucesso no âmbito da sociedade da informação." LAGARES, Rodrigo – **O Processo de Transformação da Superioridade de Informação em Superioridade de Decisão** Lisboa: Academia Militar, 2017. Dissertação de Mestrado. p. 15.

[31] "A constatação do poder e do crescimento da internet levou à suposta necessidade da sua governação", chamando à colação a lei, os órgãos de polícia criminal e, em última instância, os tribunais. "Nesta matéria identificam-se duas posições opostas: por um lado, a que defende que a governação da internet é um imperativo de segurança, sendo que esta só existe se houver regulação e controlo sancionatório. Por outro lado, a posição que defende que a governação é contranatura, assumindo-se mesmo, na vertente mais radical, como um meio de censura à própria internet. (…) A posição dominante é a da governação mínima que concilie a liberdade de cada um com a necessária privacidade, segurança e respeito pelos direitos, liberdades e garantias de cada um e de terceiros." VEIGA – ***Op cit.***

[32] *Ibidem*.

[33] **Portal de Cibersegurança da GNR** [Em Linha]. [Consult. 05 Out. 2019]. Disponível em WWW:<URL: http://portalciber.gnr.local/wordpress/index.php/2015/12/28/seguranca-na-internet/.

[34] BARBOSA, Maria – **As ameaças ao ciberespaço e a estratégia de segurança da UE e Portugal.** Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2016. Trabalho Individual. p. 7.

Em complemento, refira-se que a "segurança da informação[36] é fulcral para garantir a confiança do consumidor e o bom funcionamento do mercado interno, a fim de estimular o crescimento e o emprego"[37], uma vez que as TIC e o uso intensivo da internet têm possibilitado potenciar os índices de crescimento e qualidade de vida das populações[38]. Assim, para minimizar os riscos, deveremos adotar uma filosofia de redundância entre infraestruturas, a fim de aumentar a resiliência global do sistema[39].

Com efeito, as organizações devem "proceder a uma constante monitorização dos níveis de ameaça a que estão sujeitas, ao mesmo tempo que melhoram a sua capacidade de resposta e de proteção através da adoção de políticas internas resultantes desse mesmo processo de análise. De igual modo, não se deve perder de vista o facto de estarem sempre a surgir novas ameaças, com níveis crescentes de eficácia e perigosidade"[40].

A globalização tem permitido arquiteturar um 'novo' paradigma mundial assente na rápida evolução tecnológica. Neste sentido, verifica-se a "utilização destes mesmos recursos tecnológicos ao dispor de todos para o desenvolvimento de formas ilícitas de emprego do ciberespaço, tais como os ciberataques ou a recolha indevida de dados pessoais e das organizações[41], que se tornaram fonte de preocupações para as sociedades e um desafio para os estados modernos"[42].

---

[35] NUNES, Flávio – **Cibersegurança. "Estamos em guerra, meus senhores".** [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://observador.pt/2016/04/13/cibersegurancaestamosguerrameussenhores/.

[36] "A segurança da informação consiste em garantir que a informação existente em qualquer formato está protegida contra o acesso por pessoas não autorizadas (confidencialidade), está sempre disponível quando necessária (disponibilidade), é confiável (integridade) e autêntica (autenticidade)." SANTOS, Diana; SILVA, Rita – **Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001** [Em Linha]. Porto: Universidade do Porto, Faculdade de Engenharia, 2012. Trabalho de Segurança de Informação do MCI 2012/2013. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: https://web.fe.up.pt/~jmcruz/seginf/seginf.1314/trabs-als/final/G4-ISO.27000.final.pdf. p. 5.

[37] Tradução livre do autor. EUROPEAN COMMISSION – **Cybersecurity. Digital Agenda for Europe.** [Em Linha] [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://ec.europa.eu/digital-agenda/en/cybersecurity. p. 2.

[38] PINTO, Rui – **Novas fronteiras criadas pelos ciberataques. Um novo desafio para a cooperação internacional.** Lisboa: Instituto de Estudos Superiores Militares, 2013. Trabalho de Investigação Individual do CPOG – 2012/13. p. vi.

[39] NATÁRIO, Rui – **O Ciberespaço e a Vulnerabilidade das Infraestruturas Críticas: Contributos para um Modelo Nacional de Análise e Gestão do Risco Social.** Lisboa: Academia Militar, 2014. Dissertação de Mestrado. p. 112.

[40] RODRIGUES, Francisco – Principais ameaças no contexto da Cibersegurança. In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 48. Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2016. p. 22.

[41] Neste sentido, afigura-se como importante falar sobre os riscos inerentes ao tratamento dos dados pessoais, entre os quais destacamos: "o acréscimo constante de entidades que recolhem e tratam dados; a técnica e a crescente dificuldade de controlo dos dados pessoais – ainda que voluntariamente disponibilizados; a lei do menor esforço; a ponderação custo / benefício; a possibilidade de a informação ser utilizada contra o seu titular; a tentação securitária; a utilização de dados biométricos; a usurpação de identidade; os crimes cometidos por outros com a identidade de terceiro e a dificuldade na prova". LOURENÇO, Ana – **Os perigos da**

A massificação das TIC, "as migrações, bem como a desterritorialização do crime são fenómenos que têm suscitado acrescida preocupação por parte dos Estados, uma vez que, a par dar suas vantagens, estas acarretam uma série de desvantagens, as quais se pretende reduzir o seu impacto"[43]. Isto é, "a intensificação dos fenómenos globais, levou a uma globalização do crime, o que faz com que a criminalidade já não seja apenas de cariz nacional, passando esta a ser um problema transfronteiriço"[44].

Estes fenómenos vieram igualmente "aumentar a probabilidade de violação da privacidade do indivíduo nas suas mais diversas vertentes, bem como potencialmente expô-lo perante a comunidade"[45].

De igual modo, a (in)segurança no ciberespaço deriva da utilização massiva das TIC e do seu aproveitamento para o surgimento de novos fenómenos criminais – por exemplo, o acesso ilegítimo e a sabotagem informática –, bem como fomentou o cometimento de alguns crimes mais comuns através do ciberespaço, como é o caso do crime de injúrias.[46]

A criação do computador, em 1946, nos EUA veio revolucionar a era da informação[47]. Nesta perspetiva, Peter Drucker, na sua consagrada obra "Desafios de gestão para o século XXI"[48], refere que "o computador representa o mesmo na sociedade da informação, do que representou a máquina a vapor durante a revolução industrial"[49]. Contudo, esta "revolução da informação não se limita à criação e utilização de computadores, mas prende-se, sobretudo, com a massificação da sua utilização e da capacidade de se interligarem

---

utilização dos dados pessoais. Lisboa: Universidade Autónoma de Lisboa, 2016. Pós-graduação em Protecção de Dados Pessoais e Direito à Privacidade. Slide 16.

[42] PINTO – ***Op cit.*** p. 1-2.

[43] BRANCO, Margarida – **A importância da criação da base de dados Passenger Name Record (PNR) como meio de investigação criminal na UE.** [Em Linha]. Lisboa: Universidade Autónoma de Lisboa, 2017. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: http://hdl.handle.net/11144/3010. p. 39.

[44] *Ibidem*.

[45] A sociedade tecnológica tem suscitado "algumas graves distorções em matéria de respeito pelos direitos fundamentais, apesar de teoricamente se destinar a enriquecer a personalidade do homem, a ampliar-lhe a capacidade de domínio sobre a natureza, a aprofundar o conhecimento, a multiplicar e disseminar riqueza". RIBEIRO, Pedro – **Dados Bancários Enquanto Dados Sensíveis**. Porto: Faculdade de Direito da Universidade de Direito, 2011. Dissertação de Mestrado. p. 5.

[46] DOMINGUES – ***Op cit.***p. 15.

[47] Com o rápido desenvolvimento das TIC, a "informação tem-se tornado cada vez mais um importante recurso na vida das pessoas e, particularmente, nas atividades operacionais e estratégicas das instituições e organizações", o qual passou a ter a capacidade de "marcar a diferença entre o sucesso e o insucesso no âmbito da sociedade da informação". LAGARES – ***Op cit.*** p. 15.

[48] DRUCKER, Peter – **Management Challenges for the 21st Century.** Harper Business, 1999. ISBN: 13-978-0887309991.

[49] DOMINGUES – ***Op cit.*** p. 7-8.

em rede"[50]. Na prática, o mesmo autor advoga que o computador foi fulcral para a revolução da informação[51].

A atual estruturação das sociedades em rede é uma evidência do seu grau de desenvolvimento, pelo que se assume como uma "condição e uma necessidade não só para evoluírem, mas também para a própria sobrevivência no mundo atual"[52]. Por isso, as TIC em geral e a internet em particular são "instrumentos essenciais no quotidiano dos cidadãos, das empresas e dos Estados e a sua proteção coloca novos e grandes desafios"[53].

A par do exposto, refira-se que esta dependência do ciberespaço no nosso quotidiano acarreta o aparecimento de vulnerabilidades que devem ser mitigadas.

O aproveitamento de muitas destas vulnerabilidades acaba por conduzir ao cibercrime, o qual se limita à "criminalidade gerada especificamente através da informática usada como instrumento de trabalho e de comunicação"[54].

Neste contexto, os "serviços da sociedade da informação são essenciais no contexto das liberdades comunitárias fundamentais, nas quais assenta o mercado interno europeu, designadamente, da liberdade de circulação de bens, serviços e capitais"[55]. Deste modo, estamos perante "um mundo novo, uma sociedade nova, uma nova etapa da sociedade humana: a Sociedade da Informação"[56].

Cada dia que passa, a preocupação dos Estados passará não só pela salvaguarda da utilização segura do ciberespaço aos seus cidadãos, como pela defesa da própria soberania, tal como aconteceu na Estónia em 2007 e na Geórgia em 2008. Neste âmbito, interessa "analisar o risco social e o impacto dos diversos tipos de ciberataques, diferenciando os de

---

[50] DOMINGUES – ***Idem***.
[51] RODRIGUES, Pedro – **Segurança informática de redes e sistemas.** Vila Real: Universidade de Trás-os-Montes e Alto Douro, 2010. Dissertação de Mestrado. p. 13.
[52] PINTO – ***Op cit.*** p. 2.
[53] SANTOS, José – **Contributos para uma melhor governação da cibersegurança em Portugal.** Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2011. Dissertação de Mestrado. p. iii.
[54] Caso seja "enviada uma mensagem injuriosa, através de correio eletrónico, está preenchido o tipo penal de injúrias, não se saindo dos tipos penais comuns apesar de serem utilizados meios informáticos. No caso do cibercrime, o bem ou meio informático deve surgir como elemento típico."Assim, para este crime torna-se "necessário que o meio informático seja penalmente relevante". SIMAS, Diana – **O Cibercrime.** Lisboa: Universidade Lusófona de Humanidades e Tecnologias, 2014. Dissertação de Mestrado. p. 110.
[55] DIULIANE, Ellen – **A proteção de dados pessoais e privacidade do utilizador no âmbito das comunicações eletrónicas**. Lisboa: Universidade Autónoma de Lisboa, 2015. Dissertação de Mestrado. p. 13.
[56] "Depois da moderna era industrial iniciada pelas revoluções do século dezoito, desenvolvida pelas convicções liberais do século dezanove e aprofundada pelas aquisições sociais do pós-guerra do século vinte, chegou uma era pós-moderna cujo modelo apresenta caraterísticas e marcas que a apelidam de Sociedade da Informação." CAMPOS, Eduardo – **Acesso a dados pessoais de saúde contidos em ficheiros dos hospitais públicos: ponderação entre o direito de acesso à informação e aos documentos administrativos e o direito à protecção de dados pessoais: quem e como decide?** Lisboa: ISCTE – Instituto Universitário de Lisboa, 2009. Dissertação de Mestrado. p. 7.

motivação criminosa daqueles que, por apresentarem um maior poder disruptivo, possam colocar em risco a Segurança e Defesa do Estado"[57].

Assim, deveremos considerar a Segurança da Informação, a qual é alcançada com base na "implementação de um conjunto de controlos adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*"[58].

De acordo com o *Global Risks Report 2015*[59], editado pelo *World Economic Forum*, a probabilidade de virem a ocorrem ciberataques em 2015 estava entre os dez maiores riscos. Importa, por isso, refletir sobre os riscos tecnológicos em geral, e o de ciberataque em particular, no sentido de aumentar a consciência dos nossos decisores sobre a importância da cibersegurança, assim como da implementação de estratégias de prevenção.

De igual modo, a dependência relativamente ao ciberespaço de praticamente todos os domínios da vida "conduz ao surgimento de vulnerabilidades que têm de ser cuidadosamente analisadas e, se possível, solucionadas ou reduzidas"[60]. Com efeito, reporte-se que "a internet[61]foi criada para ser facilmente utilizada e não para a segurança, pelo que atualmente a ofensiva tem vantagem sobre a defesa. Para contrariar a evolução destes novos fenómenos têm vindo a ser desenvolvidas estratégias, medidas e iniciativas que promovem a segurança no ciberespaço"[62].

Este contexto global leva-nos a ter de considerar as ciberameaças que decorrem dos "riscos inerentes ao funcionamento num ambiente de rede aberta e perante as quais a sociedade tende a adotar uma postura mais reativa do que preventiva, uma vez que dificilmente se detetam vulnerabilidades de uma forma atempada"[63].

Os ciberataques ao governo da Estónia em 2007 são um exemplo paradigmático, nos quais ficou ilustrado o custo de se ter "uma sociedade de informação avançada, quando motivações políticas e ideológicas originaram um ciberataque sem precedentes às infraes-

---

[57] NATÁRIO – ***Op cit.*** p. 2.
[58] SERENO, José – **Tendências de implementação e segurança nas redes wireless organizacionais**. Setúbal: Instituto Politécnico de Setúbal. Escola Superior de Ciências Empresariais, 2015. Dissertação de Mestrado. p. 15.
[59] WORLD ECONOMIC FORUM – **The Global Risks Report 2015.** [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.weforum.org/reports/global-risks-report-2015.
[60] NUNES, Paulo – **Mundos virtuais, riscos reais: fundamentos para a definição de uma estratégia da informação nacional.** [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://icnsd.afceaportugal.pt/conteudo/congresso/ICNSD_4G_texto_pdf_paulo_viegas_nunes.pdf.
[61] A internet provocou uma revolução na história da humanidade, assumindo assim "uma grande relevância, quer através do setor económico criado pelo comércio eletrónico, quer através da influência cultural e educativa que ela exerce, abrindo cada vez mais possibilidades aos seus utilizadores". LEITÃO – ***Op cit.*** p. 172.
[62] DOMINGUES – ***Op cit.*** p. 16.
[63] NUNES, Paulo – **Sociedade em rede, ciberespaço e guerra de informação.** Lisboa: IDN, 2015. p. 136. e RODRIGUES – ***Op cit.***2016. p. 14.

truturas críticas daquele país, servindo em simultâneo como chamada de atenção para especialistas informáticos de todo o mundo, para as graves consequências associadas"[64].

Até ao incidente na Estónia, o paradigma das organizações alicerçava-se num patamar em que de forma isolada estas tratavam os riscos inerentes à sua atividade, nomeadamente, os relativos à cibersegurança, uma vez que estes não eram tidos em consideração num quadro sistémico e transversal. Os mesmos resumiam-se "ao desenvolvimento de soluções estandardizadas, em vez de conceberem planos ou capacidades para encetar ações coordenadas. No entanto, desde 2007, a ONU, a UE e a OTAN[65], entre outras organizações internacionais, introduziram novas políticas de cibersegurança ou reviram as antigas"[66].

As ameaças[67] no ciberespaço são parecidas com aquelas que conhecemos no mundo real, tais como: crime, espionagem, ativismo, terrorismo.[68]

Neste sentido, constatamos que não existe uma definição comum de ciberameaças, devido a cada Nação as caraterizar de forma distinta. No entanto, podemos diferenciá-las utilizando a metodologia da *International Telecommunication Union* (ITU), que as classifica segundo as suas caraterísticas, impactos, origens e atores: podem ser "acidentais", se não houve premeditação, por exemplo no caso de uma falha de *software* involuntária; serão "intencionais", com vários graus de sofisticação, sempre que exista uma vontade de atacar; as ameaças "ativas" modificam o estado ou operação de um sistema enquanto as "passivas" não afetam o sistema, mas recolhem informação.[69]

Como tal, e a fim de mitigar estas ciberameaças, começou a ser desenvolvida uma multiplicidade de "ferramentas[70] para identificar e defender-se contra *software* malicioso, embora poucas nas ciências sociais tenham explorado os fatores ambientais e sociais que

---

[64] Casos posteriores, como "o *worm* que atacava o Microsoft Windows e os ciberataques contra a Google na China em 2010, mostram o grau crescente de sofisticação do cibercrime." SILVA, Nuno – **Segurança e Defesa Nacional: o desenvolvimento de capacidades de Ciberdefesa.** Lisboa: Instituto de Estudos Superiores Militares, 2012. Trabalho de Investigação Individual do CEMC – 2011/12. p. 17.

[65] *North Atlantic Treaty Organization.* Traduzido: Organização do Tratado do Atlântico Norte (OTAN).

[66] "Também no plano legal houve necessidade de adaptação às novas ameaças, uma vez que estas põem à prova os limites da legislação existente, sobre proteção da informação, comunicações eletrónicas e de acesso às informações públicas." SILVA – ***Op cit.*** p. 17.

[67] "Uma ameaça é qualquer perigo potencial para a informação ou para os sistemas, que ocorre quando algo ou alguém identifica uma vulnerabilidade específica e a utiliza". HARRIS, S. – **All in one CISSP exam guide.** 5th Ed. McGraw-Hill, 2010. p. 54.

[68] ROBINSON, et al – **Cyber-security threat characterisation.** RAND Europe, 2013. p. 5.

[69] WAMALA, F. – **The ITU National Cybersecurity strategy guide.** International Telecommunication Union, 2011. e ANTUNES– ***Op cit.*** p. 10.

[70] "As ferramentas automatizadas permitem que invasões de sistemas remotos sejam feitas em poucos segundos, o que facilita o lançamento de ataques na internet e o rastreamento cada vez mais difícil." Tradução livre do autor. NICKOLOV, Eugene – **Critical information infrastructure protection: analysis, evaluation and expectations.** [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.comw.org/tct/fulltext/05nickolov.pdf. p. 107.

podem afetar a criação e a distribuição de *malware*"[71], não obstante a insuficiência de dados disponíveis sobre a origem dos respetivos programadores e ao elevado número de *softwares* criados mundialmente por *hackers*[72].

Por outro lado, a OTAN definiu no seu conceito estratégico aquelas que considera como as atuais ameaças, as quais são: "a convencional, incluindo mísseis balísticos; a proliferação de armas de destruição massiva, incluindo armas nucleares; o terrorismo, que coloca uma ameaça direta à segurança dos cidadãos; a instabilidade além-fronteiras dos países da OTAN, que potencia extremismos e atividades ilegais; os ciberataques, cada vez mais frequentes, melhor organizados e com maior efeito destrutivo; a dependência energética, que pode estar exposta a disrupções, das comunicações e dos transportes; as dependências tecnológicas, incluindo armamento laser, guerra eletrónica e tecnologias que impeçam o acesso ao espaço e os constrangimentos ambientais e de recursos, incluindo riscos de saúde, escassez de água e necessidade de energia"[73].

Neste contexto, a cifragem vê o seu papel reforçado, uma vez que ao contrário do que sucedia "até à década de 1990, em que a cifragem era um recurso técnico destinado ao uso por militares, por serviços de informação e por grandes empresas, hoje, a generalidade dos utilizadores das redes de informação, processamento e comunicação tem acesso livre a esta tecnologia de segurança presente em vários produtos comerciais"[74].

Numa perspetiva mais jurídica, verificamos que a legislação penal tem ainda alguma dificuldade em se adaptar a este novo contexto tecnológico, uma vez que "o direito não consegue acompanhar o avanço das novas tecnologias em especial a internet, [sendo que] é justamente neste ambiente livre e sem fronteiras que se desenvolveu uma nova modalidade

---

[71] Tradução livre do autor. BURRUSS, George; HOLT, Thomas; BOSSLER, Adam – Exploring the Utility of Open Source Data to Predict Malicious Software Creation. **Cyber Infrastruture Protection.** Vol. II. U.S. Army War College Press. 2013. ISBN 1-58487-571-2. p. 183.

[72] Exemplos de atividades realizadas por *hackers*: "ataques a sistemas com perímetros inseguros, uso de páginas de terceiros para propaganda nacionalista, bombas de *emails* que sobrecarregam servidores de organizações contra as quais eles estão a protestar, computadores *zombie's* implantados na internet, que servem como controles remotos para ataques". Em alguns países, até o governo está envolvido na "preparação e execução de ataques cibernéticos." Tradução livre do autor. NICKOLOV – ***Op cit.*** p. 108.

[73] SANTOS, Henrique – ***Soft Power* e *Hard Power*: dicotomia ou complementaridade.** Lisboa: Instituto de Estudos Superiores Militares, 2015. Trabalho de Investigação Individual do CPOG – 2014/15. p. 9.

[74] Recordemos que "a cifragem, que começou por conhecer uma aplicação destinada à proteção e autenticação de comunicações eletrónicas, agora implodiu na sua utilização prática, permitindo impedir de forma aberta ou de forma dissimulada o acesso a informação estática armazenada em diferentes tipos de memórias de massa". BRAVO, Rogério – **Dos vestígios em ambiente digital à prova digital como intelligence.** [Em Linha]. 2009. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.academia.edu/4691991/DOS_VEST%C3%8DGIOS_EM_AMBIENTE_DIGITAL_%C3%80_PROVA_DIGITAL_COMO_INTELLIGENCE. p. 8.

de crimes, uma criminalidade virtual desenvolvida por agentes que se aproveitam da possibilidade do anonimato e da ausência de regras na rede mundial de computadores"[75].

Nesta arquitetura do ciberespaço, as ameaças sofreram uma mutação, no sentido de que estas já não são apenas provenientes dos entusiastas da computação [*hackers*] que invadem os sistemas de TI em busca do conhecimento ou da notoriedade, mas de oponentes muito mais dedicados: criminosos, terroristas e Estados competidores.[76]

As ameaças que resultam do ciberespaço são variáveis consoante a vontade ou os seus objetivos, podendo estas serem consideradas como as principais ameaças: "o cibercrime, o *hacktivismo*, o ciberterrorismo, a ciberguerra, o crime organizado e a espionagem"[77]. Deste modo, o "principal desafio a nível do Estado é a aplicação de medidas de segurança que garantam a resiliência do ciberespaço, desenvolver a política e as capacidades no domínio da ciberdefesa no quadro das forças e serviços de segurança (FSS), desenvolver os recursos industriais e tecnológicos para a cibersegurança"[77].

Focando-nos agora em Portugal, podemos afirmar que no interior do nosso território existem "diversos cabos de telecomunicações e infraestruturas de informação, materializando os milhares de ligações transnacionais que permitem dar suporte à internet"[78], não obstante existir "uma falta de perceção sobre a natureza e limites do ciberespaço, caraterizado pela indefinição de fronteiras tais como se conhecem na sua expressão física ou geográfica. Esse facto, gera a dificuldade de definir a maneira pela qual um Estado pode exercer a sua soberania sobre uma área ou ambiente que não domina e não controla"[79].

Deste modo, e de acordo com a motivação associada aos ataques deliberados, podemos agrupar as ameaças em:

• Cibercrime: as ameaças são "centradas essencialmente na obtenção de benefícios económicos através de ações ilegais. As ações relacionadas com a fraude bancária, com cartões de crédito ou a realização de transações em diferentes páginas *web*, constituem exemplos de ações comuns relacionadas com este tipo de ameaças"[80].

---

[75] MENEZES, Umbelina – **O Papel das Forças e Serviços de Segurança no Combate aos Crimes Cibernéticos em Angola.** Lisboa: Universidade de Lisboa, Faculdade de Direito, Instituto Superior Técnico, 2016. Dissertação de Mestrado. p. 23.

[76] Estes "oponentes não estão interessados em fama ou em satisfazer o ego, em vez disso, são motivados por interesses políticos, ideológicos e financeiros muito mais poderosos. Atualmente, as organizações terroristas usam o ciberespaço em atividades de apoio às suas ações, como o recrutamento, levantamento de fundos, propaganda, treino e planeamento das suas atividades". MENEZES – ***Op cit.*** p. 24.

[77] *Ibidem*.

[78] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 16.

[79] *Ibidem*.

[80] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 22.

• Ciberespionagem: o foco é a "obtenção de informações, seja para benefício próprio ou para deter um benefício monetário posterior com a sua venda. A informação mais suscetível de identificar-se neste campo pode pertencer, nomeadamente, a um governo ou até a organizações privadas, e ser classificada, sendo esta uma mais-valia para os atacantes"[81].
• Ciberterrorismo: procura-se um "impacto social e político significativo pela destruição física"[82], constituindo as infraestruturas críticas (IC) os alvos de ataque mais prováveis.
• Ciberguerra: pode-se definir como "uma luta ou conflito entre duas ou mais nações ou entre diferentes fações dentro de uma nação onde o ciberespaço é o campo de batalha"[83].
Finalmente, o "hacktivismo ou ciberativismo, pelo seu impacto crescente também tem vindo a assumir-se como um campo de ação da ciberameaça"[84].

De acordo com o art.º 35º da Constituição da República Portuguesa (CRP), e considerando o Direito da Cibersegurança, poderemos elencar duas conclusões: "por um lado, a proteção dos direitos fundamentais das pessoas frente ao uso da informática, proverbialmente antecipado pela CRP logo em 1976, assunto que se reforçou com a nova legislação europeia e interna aprovada; por outro lado, a proteção da comunidade política que seja empreendida através de estruturas de segurança nacional dedicadas a combater as ciberameaças, as quais podem assumir uma variedade apreciável"[85].

Nesta perspetiva, outro aspeto a ter em conta prende-se com a necessidade de refletir sobre a relação entre proteção de dados e partilha de informação. Assim, a intenção de aumentar a segurança terá de ser relacionada com o benefício do uso da internet e as expetativas dos cidadãos, de acordo com a política governamental de proteção de dados e preservação da privacidade. Aqui, refira-se que "as empresas de todos os tipos confiam na disposição de consumidores e parceiros de negócios de lhes fornecer informações privadas. Esses componentes, por sua vez, esperam que essa informação permaneça privada e segura"[86], ou seja, os cidadãos esperam proteção contra intrusões por parte de atores privados e governamentais[87].

---

[81] *Ibidem*.
[82] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 23.
[83] *Ibidem*.
[84] *Ibidem*.
[85] GOUVEIA, Jorge – **Direito da Segurança. Cidadania, Soberania e Cosmopolitismo.** Coimbra: Almedina Editora, 2018. 1ª Ed. ISBN 978-972-40-7492-4. p. 920.
[86] Tradução livre do autor. HATHAWAY, Melissa; KLIMBURG, Alexander – The Five Mandates of National Cyber Security. In **National Cyber Security Framework Manual.** NATO CCD COE Publication, Tallinn 2012. ISBN 978-9949-9211-2-6. p. 39.
[87] Refira-se aqui que, remonta ao ano de 1980, o momento em que "a OCDE publicou uma 'Recomendação sobre diretrizes que regem a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais'. As

Para tal, verifica-se a necessidade de troca atempada de informações e alertas entre entidades privadas e públicas, com o intuito de combater a criminalidade e outras atividades ilícitas no ciberespaço, mesmo que para cumprir este objetivo seja necessária a troca de dados confidenciais que podem ser abrangidos por essas leis de privacidade e proteção de dados. Todavia, as "leis nacionais podem ser insuficientes, por si só, para fornecer aos cidadãos proteções de privacidade além das fronteiras e, ao mesmo tempo, permitir a troca oportuna de informações sobre ameaças"[88].

O funcionamento em rede terá de ser capaz de garantir a segurança e a proteção das infraestruturas essenciais ao normal funcionamento da vida em sociedade, as designadas infraestruturas críticas, pelo que, "importa refletir sobre as principais envolventes da utilização da informação, em particular, o desenvolvimento de uma Estratégia da Informação[89] Nacional e o levantamento de um sistema de proteção das infraestruturas de informação capaz de promover a livre utilização e garantir a segurança do ciberespaço"[90].

Nesta perspetiva, o ciberespaço assumiu-se como o quinto domínio da guerra tradicional, juntando-se aos já existentes domínios da guerra tradicionais, como o marítimo, o terrestre, o aéreo e o espacial.[91]

Este novo domínio constitui-se como um "cenário para novos desafios, onde se podem desenvolver todo o tipo de atividades num mundo virtual com consequências bem reais, alavancadas pelas caraterísticas únicas deste novo ambiente"[92], sendo que todas as dimensões são interdependentes, considerando que os nós físicos do ciberespaço podem

diretrizes da OCDE influenciaram os acordos internacionais, as leis nacionais e as políticas de autorregulação". Tradução livre do autor. HATHAWAY – ***Op cit.*** p. 39-40.

[88] Tradução livre do autor. HATHAWAY – ***Op cit.*** p. 40-41.

[89] Sobre a "Guerra de Informação", para um maior conhecimento sobre os problemas e fragilidades existentes em Portugal, bem como identificação de quais as medidas que devem ser tomadas de um modo sistémico e cronológico para colmatar as nossas lacunas e reduzir as fraquezas existentes ao nível do desenvolvimento da Estratégia da Informação, nas suas componentes estrutural, genética e operacional, consultar NUNES, Paulo – **Sociedade em rede, ciberespaço e guerra de informação: contributos para o enquadramento e construção de uma estratégia nacional de informação.** 2.ª Ed. Lisboa: Instituto da Defesa Nacional, 2016. ISBN 978-972-9393-34-1.

[90] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 8.

[91] Na Defesa, "a terra, o mar, o ar e o espaço têm constituído os domínios tradicionais de desenvolvimento das operações militares e, por conseguinte, é neles que se têm centrado os esforços relacionados com a obtenção de capacidades militares. No entanto, o ciberespaço já foi definido e aceite como o quinto domínio operacional, no qual se levam a cabo operações militares específicas e em relação ao qual as operações militares que se desenvolvem nos outros domínios dependem cada vez mais." INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 11. e NATÁRIO – ***Op cit.*** p. 1.

[92] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 11.

residir e se projetar com grande influência e impacto, em todas as outras, bem como as atividades que se processam nele.[93]

Até recentemente, "a orientação no campo da Defesa em matéria de proteção do ciberespaço, era essencialmente de natureza reativa e estática, focada na defesa dos sistemas de informação e telecomunicações, através da implementação de medidas preventivas, de deteção e de recuperação de diferente natureza (físicas, pessoal, técnicas, etc.)"[94].

Esta abordagem é habitualmente caraterizada como *Information Security*[95] (INFOSEC). Todavia, e considerando a natureza dinâmica do próprio ciberespaço, estas medidas "INFOSEC, apesar de necessárias, já não resultam atualmente numa aproximação suficientemente forte para proporcionar um nível de proteção adequado, no que à segurança da informação se refere"[96]. Deste modo, surge o conceito de ciberdefesa, o qual procura "agrupar o conjunto de medidas e ações que se adaptam a este novo ambiente de informação dinâmico e que são capazes de proporcionar a proteção da informação e os sistemas que agora passam a ser geridos também de acordo com este novo cenário operacional"[97].

Esta nova abordagem concretiza uma ampliação "dos serviços de segurança a proporcionar no próprio ciberespaço, não apenas focado na proteção da disponibilidade, integridade e confidencialidade, mas também incluindo serviços como autenticação, rastreabilidade e não-repúdio"[98].

De igual modo, surge a necessidade de proteger as infraestrutura de informações críticas, tendo sido definidos "três objetivos estratégicos: impedir ataques cibernéticos contra infraestruturas críticas; reduzir vulnerabilidades nacionais a ataques cibernéticos; e minimizar danos e tempo de recuperação de ataques cibernéticos que ocorrem"[99].

---

[93] Para um aprofundamento deste tema consultar FM 3-38 – **Cyber Electromagnetic Activities**, p. 8. e FRIAS, Oscar – **Cyber Intelligence. A obtenção de informações a partir de fontes abertas no Ciberespaço.** Lisboa: Academia Militar, 2013. Dissertação de Mestrado. p. 1.

[94] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 11.

[95] A nível internacional, quando nos referimos à segurança da informação e do ciberespaço, os termos frequentemente usados são normalmente expressos em inglês (*information assurance cyber security*, *infosec*, *computer security*, *computer networks security*, *computer networks defence*, *cyber defence*, *critical information infrastructure protection*, (…)), mas geralmente o seu significado tem diferentes matrizes, dependendo do país de origem e de quem os usa. Neste âmbito, verifica-se que nem sempre é possível encontrar concordância com a tradução direta dos termos anglo-saxónicos que os compõem. Em Espanha assume a designação de STIC (*Seguridad de las Tecnologías de la Información y las Comunicaciones*) e em Portugal a designação de Segurança da Informação. INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 11.

[96] *Ibidem*.

[97] *Ibidem*.

[98] *Ibidem*.

[99] Para atingir esses objetivos, é necessária uma nova estratégia. Uma que incorpore mais do que apenas as questões tecnológicas e inclua os seguintes elementos: tomar medidas preventivas em todos os níveis; melhorar a deteção precoce e as capacidades de reação rápida, tanto para controlo de danos quanto para a busca dos culpados; limitar o impacto de interrupções no governo e na sociedade; garantir que os sistemas afetados

Outro passo importante foi dado com a Diretiva relativa à segurança das redes e da informação (Diretiva NIS). Esta Diretiva ao reforçar a preparação, a cooperação transfronteiriça e o intercâmbio de informações, permite aos cidadãos colher todos os benefícios que o ambiente digital oferece, bem como permitir ao setor público e privado confiar nos serviços das redes digitais a nível nacional e da UE[100]. Esta estratégia aborda a cooperação internacional como uma prioridade fundamental, devido à interconexão dos sistemas de rede e informação, fatores que potenciam a cibersegurança para uma dimensão global.[101]

No domínio do ciberespaço falamos da "internet e de como a necessidade exponencial de troca e partilha de informação deu origem a serviços, agora segregados na denominada "computação em nuvem", que potenciam a vantagem competitiva das empresas, desenvolvendo áreas como o *eCommerce*, *eGovernment*, *eBusiness* e *eStrategy*"[102].

A acrescentar a estes dados, acrescente-se o facto de estarmos a assistir a uma mudança de paradigma da *Internet of Things (IoT)* para a *Internet of Everything (IoE)*, levando este fenómeno a uma hiper conetividade que, mais uma vez, tem tanto de desafiante, como de assustador e perigoso, nomeadamente em termos de segurança da informação.

Em complemento, refira-se que a sociedade está permanentemente a aumentar a rede na qual se encontra apoiada, sendo uma evidência de tal "o aumento considerável do número de dispositivos a partir dos quais podemos aceder à internet, principalmente dos dispositivos móveis, como é o caso dos *smartphones* e *tablets*"[103]. Presentemente, a discussão centra-se no fenómeno da *IoE*[104], um conceito criado no início do terceiro milénio por Kevin Ashton, e que se baseia na ideia de existir uma poupança de trabalho e tempo, caso "todos os nossos objetos pessoais estivessem ligados em rede, pudessem comunicar uns com os outros e serem ativados e geridos por meio informático"[105].

Neste sentido, em 2018 estimava-se que aproximadamente 10 biliões de "coisas" estivessem conetadas à internet, variando de computadores a IC, e eletrodomésticos. A

---

continuem a funcionar num nível mínimo ou possam ser restaurados no menor tempo possível. Tradução livre do autor. NICKOLOV – ***Op cit.*** p. 108.

[100] Ao estabelecer incentivos para promover investimentos, transparência e conscientização dos utilizadores, a estratégia aumentará a competitividade, o crescimento e o emprego na UE.

[101] Tradução livre do autor. EUROPEAN COMMISSION – **Cybersecurity. Digital Agenda for Europe.** [Em Linha] [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://ec.europa.eu/digital-agenda/en/cybersecurity. p. 3.

[102] FRIAS – ***Op cit.*** p. 1.

[103] DOMINGUES – ***Op cit.*** p. 10.

[104] "As sociedades, totalmente mergulhadas numa lógica de funcionamento em rede, encontram-se dependentes do ciberespaço. Com a *"Internet of Things",* com o desenvolvimento das redes de comunicações, com a globalização económica, com o conceito de "cidades inteligentes", esta tendência tende a crescer, tal como os riscos daí resultantes." RODRIGUES – ***Op cit.*** 2016. p. 4.

[105] DOMINGUES – ***Op cit.*** p. 7-8.

tendência será a de um aumento substancial nos próximos anos, pelo que a "CISCO projeta que, pelo menos, 50 biliões[106] de coisas possam estar conetadas à internet até 2020"[107].

1.1.2. O Ciberespaço

"Não há dúvida de que o ciberespaço, como um ambiente virtual onde se agrupam e relacionam utilizadores, linhas de comunicação, *sites*, fóruns, serviços de internet e outras redes, tornou-se um novo "espaço", que a par dos tradicionais domínios da interação humana como a terra, o mar, o ar e o espaço, é o meio onde se desenvolvem as atividades económicas, produtivas e sociais das nações mais desenvolvidas. O ciberespaço toca praticamente tudo e todos. Proporciona uma plataforma para a inovação e prosperidade, e os meios para melhorar o bem-estar geral de todo o mundo."[108]

O conceito de ciberespaço varia de autor para autor, de acordo com a sua abordagem concetual, não existindo uma definição que seja consensual quer a nível nacional ou internacional[109].

Recuando no tempo até 1982, encontramos o vocábulo ciberespaço que foi idealizado por William Gibson, um escritor de ficção científica, que o utilizou pela primeira vez à data num pequeno romance de sua autoria, intitulado de "Neuromancien"[110], onde se faz referência a um espaço virtual composto por cada computador e usuários conetados numa rede à escala mundial."[111]

Como já vimos, o espaço cibernético intensificou transformações sociais nos mais diversos domínios da atividade humana, pelo que Manuel Castells apelida esta factualidade de sociedade em rede[112]."[113]

---

[106] De acordo com a UE estima-se que 50 biliões de dispositivos e objetos serão conectados à internet até 2020; o mercado global de cidades inteligentes seja da ordem de 1,5 trilião de euros e cresça 17% a cada ano; nos próximos 10 anos, as cidades serão os maiores geradores / usuários da *IoT* que beneficiarão diretamente os cidadãos nas suas vidas diárias. Alguns exemplos: mobilidade conetada e sustentável, sistemas de saúde, monitorização e gestão ambiental da água, energia e outros recursos e vida cultural, entre outros.

[107] Tradução livre do autor. LINDSTROM, Gustav – Desafios emergentes de segurança cibernética. In DEFENCE, Federal Ministry Republic of Austria – **Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union.** Vol. V. 1ª Ed. Luxembourg: Publications Office of the European Union, 2018. ISBN 978-92-95201-12-5.p. 159.

[108] INSTITUTO DE DEFESA NACIONAL – ***Op cit.*** p. 8-9.

[109] "Tal como noutros termos afins como sejam cibernauta, ciberguerra ou ciberarma, o prefixo "ciber" apela ao imaginário do virtual e transporta o recetor para o contexto das TIC. Diferentes setores da sociedade usam o termo ciberespaço para se referirem a coisas tão distintas como a rede planetária de computadores, a possibilidade de realizar atividades através da internet, ou o armazenamento de informação na *cloud*, pelo que, numa perspectiva abrangente, podemos definir ciberespaço como o conjunto "[d]as diferentes vivências do espaço associado às tecnologias e à computação"." GUEDES, Armando; SANTOS, Lino – Breves reflexões sobre Poder e Ciberespaço. In **Revista de Direito e Segurança**. N.° 6 (julho / dezembro de 2015). p. 190.

[110] GIBSON, William – **Neuromancien.** Paris: La Découverte, 1985. p. 64.

[111] LEITE, Ana – A problemática da cibersegurança e os seus desafios. In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 49. Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2016. p. 3.

[112] CASTELLS, Manuel – **A Sociedade em Rede. A Era da Informação: Economia, Sociedade e Cultura.** [Em Linha]. Vol. I. Fundação Calouste Gulbenkian CERT-EU. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://cert.europa.eu/cert/plainedition/en/cert_about.html.

[113] LEITE – ***Op cit.*** p. 4.

De igual modo, o ciberespaço constitui-se como um novo domínio, considerando que permite ser utilizado ou para o confronto direto no ciberespaço ou como mais uma forma de fazer a guerra.

O grande aumento da interligação dos sistemas informáticos ocorrido desde o final da Guerra Fria, particularmente da internet, revolucionou a forma como os governos, as empresas e os indivíduos comunicam e fazem negócios. No entanto, este advento de um mundo hiperligado trouxe também enormes riscos para os sistemas, para os computadores e, mais importante ainda, para o normal funcionamento das IC que eles suportam. Embora a definição exata daquilo que é considerado crítico varie de país para país, há um fio condutor que liga todas as conceções sobre o assunto: a sua importância para o funcionamento normal da sociedade[114].

O "ciberespaço, enquanto espaço de defesa de interesses, impõe novas formas de interação e de relacionamento entre as Unidades Políticas"[115]. Desta forma, "as estratégias prosseguidas centram-se no valor dos recursos de informação e em operações destinadas a afetar esse valor, onde se privilegia o princípio da economia de meios e a ação indireta"[116]. Assim, "estamos perante uma situação paradigmática da relação bem-estar/desenvolvimento e segurança das sociedades onde um mundo sem fronteiras como o ciberespaço cria tantas oportunidades como riscos"[117].

Como tal, o ciberespaço tem sido um tema de debate e "profunda investigação por parte, não só das forças de segurança mas também das agências de *Intelligence*, devido às novas ameaças de caráter transnacional que começaram a surgir e a adquirir um certo relevo na comunidade internacional nos últimos anos"[118].

Considerando o ciberespaço "como uma plataforma sem fronteiras que permite a interação de qualquer pessoa para os mais diversos fins (…) impõe-se a necessidade de criar estruturas nacionais e internacionais de monitorização e de prevenção de práticas que coloquem em causa a segurança interna e externa dos Estados"[119].

---

[114] NATÁRIO, Rui; NUNES, Paulo – Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. In **Revista Militar** N.º 2547 (04-2014). p. 249-286.
[115] Para um aprofundamento deste tema consultar NUNES, Paulo – **Mundos virtuais, riscos reais: fundamentos para a definição de uma estratégia da informação nacional.** Disponível em: http://icnsd.afceaportugal.pt/conteudo/congresso/ICNSD_4G_texto_pdf_paulo_viegas_nunes.pdf.
[116] *Ibidem.*
[117] *Ibidem.*
[118] Estas ameaças físicas podem ser definidas como: "o crime organizado, o terrorismo, o tráfico de seres humanos, que se têm evidenciado em todo o mundo devido às globalização e aos impactos que esta tem tido na vida em Sociedade dos Estados". RODRIGUES – ***Op cit.*** 2016. p. 3.
[119] LEITE – ***Op cit.*** p. 1.

Deste modo, não é de "estranhar que os governos manifestem a intenção de defender os ativos e interesses estratégicos dos seus países nesse âmbito"[120]. Como tal, na "Estratégia Internacional para o ciberespaço", assinada pelo à data presidente dos EUA, Barack Obama, podemos ler: "Todos os Estados têm o direito inerente de legítima defesa e de reconhecer que certos atos hostis realizados no ciberespaço podem obrigar a tomar ações no âmbito dos compromissos que temos com os nossos aliados militares. Reservamo-nos o direito de usar todos os meios necessários: diplomáticos, informacionais, militares e económicos, adequados e consistentes com o direito internacional aplicável, a fim de defender a nossa nação, os nossos aliados, os nossos parceiros e os nossos interesses"[121].

Vejamos agora as definições de ciberespaço consideradas nos seguintes países: segundo o Dicionário da Real Academia Espanhola (DRAE), "ciberespaço" é o "ambiente artificial criado por meios informáticos", enquanto "cibernauta" é a "pessoa que navega por ciberespaços". Não encontramos na DRAE a definição de "cibersegurança"ou "ciberdefesa", mas podemos encontrar que o prefixo "*cyber*" é um elemento composto que significa "cibernético" e vem da palavra "cibernética". Esta, por sua vez, faz referência ao "estudo das analogias entre os sistemas de controlo e comunicação dos seres vivos e os das máquinas e, em particular, carateriza a aplicação dos mecanismos de regulação biológica e tecnológica". Este termo apresenta uma definição similar no Dicionário *Houaiss* da Língua Portuguesa. Etimologicamente, o termo vem do francês (*cibernétique*), que por sua vez o adotou do inglês (*cybernetics*), mas tem origem no grego (*κυβερνητικ*), onde ele se refere à "arte de governar um navio". Assim, podemos concluir que a "cibersegurança" se refere à "segurança cibernética", assim como a "ciberdefesa"se refere à "defesa cibernética".[122]

Mas afinal o que se entende por ciberespaço? Não obstante a dificuldade de conseguirmos ter um conceito universal tão reclamado por todos e que tão útil seria, tanto mais que falamos de um conceito que perpassa diversas realidades, a verdade é que encontramos igual dificuldade em outros campos do saber, nomeadamente na definição de terrorismo ou de *Intelligence.* Não alheio a esta dificuldade está seguramente o facto de existirem diversas comunidades, com perspetivas distintas a trabalhar sobre o mesmo objeto.

A noção de ciberespaço pode então ser definida como:

[120] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 9.
[121] *Ibidem*.
[122] *Ibidem*.

- "A rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores"[123];

- O ciberespaço contempla "inúmeros computadores interconectados, servidores, *routers, switches* e cabos mas é este emaranhado tecnológico que serve de suporte, tecnologicamente, às infraestruturas críticas (...) e a muitos serviços críticos"[124];

- O ciberespaço "designa hoje a rede global de infraestruturas de tecnologias de informação interligadas entre si, especialmente as redes de telecomunicações e os sistemas de processamento dos computadores"[125].

Assim, e voltando à necessidade de procurarmos definir o conceito de ciberespaço, acolhemos para nós esta definição por nos parecer que, de entre as várias consultadas, era a que melhor se adaptava à perspetiva da segurança da informação: o ciberespaço consiste "em artefactos baseados em/ou dependentes das tecnologias da comunicação e computação; a informação que esses artefactos usam, armazenam, manuseiam ou processam; e as interconexões entre esses vários elementos"[126].

Neste sentido, e optando por uma vertente mais técnica, o ciberespaço pode ser definido como "um conjunto de redes e sistemas de comunicação que estão interligados, entre si de forma direta ou indireta"[127]. Para além da sua componente tecnológica, deveremos encarar o ciberespaço noutras dimensões, ou seja, "as vulnerabilidades inerentes ao seu emprego e ameaças que possam afetá-los, como os fatores humanos, uma vez que são estes que caraterizam os utilizadores deste ambiente. Para se poder entender adequadamente o seu funcionamento e os seus riscos, deve-se prestar especial atenção às pessoas que acedem ao ciberespaço assim como com as suas diferentes culturas e motivações"[128].

Por outro lado, as tecnologias computacionais permitiram o surgimento de uma dimensão virtual, na qual o ciberespaço permite a criação de "uma nova dimensão, quer de

---

[123] FERNANDES, Filipe – **A Cibersegurança e as Estruturas Críticas: A GNR. Ciberguarda, o Futuro.** Lisboa: Academia Militar, 2013. Dissertação de Mestrado.
[124] DOMINGUES – ***Op cit.*** p. 59.
[125] MACHADO, Paulo – **O papel da GNR no contexto da Cibersegurança Nacional.** Lisboa: Instituto Estudos Superiores Militares, 2015. p. 6.
[126] Para um maior aprofundamento do tema recomenda-se a consulta de CLARK, David; BERSON, Thomas; LIN, Herbert – **At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.** Washington D.C. The National Academies Press, 2014. Cfr. Capítulo 8 "O Ciberespaço: Desafios Segurança e à Estratégia", do livro CALDAS, Alexandre; FREIRE, Vicente – **Segurança Internacional: Perspetivas Analíticas.** Lisboa: Imprensa Nacional – Casa da Moeda/Instituto da Defesa Nacional, 2013.
[127] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 10.
[128] *Ibidem*.

oportunidades e imprevisibilidades mas também um novo espaço de conflitos"[129], considerando a sua constante evolução e a frequência das suas mudanças.

Nesta perspetiva, importa ainda considerar as particularidades do ciberespaço, com o intuito de melhor conseguirmos identificar o seu relevo nos âmbitos da segurança e defesa, em particular das seguintes características[130]: caráter dinâmico[131]; custo irrelevante de acesso[132]; enorme potencial de crescimento[133]; alta capacidade de processamento[134]; caráter assimétrico[135]; anonimato[136]; alta capacidade para produzir efeitos físicos[137]; e transversalidade[138].

Todas estas caraterísticas[139] levam a que, para além do perigo das ameaças externas por parte de outros Estados, hoje em dia, com a existência das redes de comunicação e do ciberespaço, se assuma que "a segurança adota outros termos e dimensões que vão para lá do espaço físico e imediato"[140].

No seguimento, surge outra definição de ciberespaço que consiste no "conjunto dos sistemas informáticos como o *hardware*, *software*, redes de comunicação, equipamentos e meios de comunicação e informação neles processados e armazenada"[141].

Em complemento, não olvidemos que "as formas de comunicação virtuais suplantaram os meios de comunicação social tradicionais, na medida em que a informação circula

---

[129] SILVA, Susana – **A Ciberespionagem no contexto Português.** Lisboa: Academia Militar, 2014. Dissertação de Mestrado. p. 30.
[130] *Ibidem*.
[131] "O Ciberespaço tem uma frequência de mudança elevada. Os diferentes sistemas que o integram, mudam e modificam-se constantemente, especialmente as suas interligações. As vulnerabilidades são descobertas quase diariamente e as ameaças emergentes surgem e mudam constantemente."
[132] "Hoje em dia a barreira económica de acesso ao Ciberespaço é muito pequena, estimando-se que atualmente mais de um terço da população mundial tenha acesso à internet."
[133] "Tanto a nível de funcionalidades como de velocidade de troca de informação."
[134] "Capacidade elevada de procura, processamento e também de armazenamento de informação."
[135] "Neste novo domínio, com muito poucos recursos podem-se desenvolver ações hostis de grande impacto. A assimetria revela-se tanto ao nível dos recursos como do conhecimento necessário para desenvolver essas ações."
[136] "É muito difícil detetar e seguir a origem de um ataque, o que dificulta a capacidade de dissuasão e resposta."
[137] "Refletida na possibilidade de atingir uma ampla gama de indústrias e dispositivos."
[138] "Uma ação ou evento ocorrido no ciberespaço pode afetar um ou mais domínios de atividade das modernas sociedades, como sejam a área política, económica, social ou mesmo a segurança e defesa dos Estados."
[139] "Acrescentemos ainda as caraterísticas como a velocidade com que a informação circula pelo globo, a quantidade de dados que é possível armazenar e partilhar, o facto de ser um lugar aterritorial e sem fronteiras físicas definidas, ao mesmo tempo que se torna um lugar comum pelo fácil acesso ao mesmo torna esta realidade ainda mais complexa e difícil de compreender." BARBOSA – ***Op cit.*** p. 4.
[140] BARBOSA – ***Op cit.*** p. 3.
[141] FERNANDES, Filipe – **A Cibersegurança e as Estruturas Críticas: A GNR. Ciberguarda, o Futuro.** Lisboa: Academia Militar, 2013. Dissertação de Mestrado. p. 90. e GINKEL, B. – **Responding to Cyber Jihad: Towards an Effective Counter Narrative.** 2015.

de forma mais rápida e atualizada na internet, ao mesmo tempo em que há outros atores a produzi-la e partilhá-la, não sendo necessariamente produtores formais de informação"[142].

Noutra perspetiva consideremos agora as IC, as quais se encontram nos sistemas de satisfação de necessidades básicas da população, as quais utilizam e dependem do ciberespaço para prosseguirem tal objetivo, sendo alguns exemplos os sistemas de gestão e abastecimento de eletricidade e água potável ou sistemas financeiros, de transportes ou telecomunicações. Toda esta "dependência resulta da forte utilização de aparelhos tecnológicos e digitais que utilizam a rede para comunicarem e funcionarem"[143].

Uma Infraestrutura Crítica[144] Nacional, nos termos do Decreto-Lei n.º 62/2011 de 9 de maio, considera-se como "a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções[145]".

Deste modo, um qualquer ciberataque ao "funcionamento ou instalações destas infraestruturas terá repercussões na sociedade civil, assim como nos níveis políticos e militares da mesma, na medida em que serão afetados aspetos importantes ao seu funcionamento, concretizando-se estes ataques numa questão de segurança nacional"[146].

As TIC e as suas vulnerabilidades têm permitido a pequenos Estados, e mesmo a atores não Estatais, "aspirar a reduzir assimetrias com as principais potências mundiais e a ver melhoradas as suas relações de poder na cena internacional"[147].

Nesta perspetiva, refira-se que "o ciberespaço não irá substituir o espaço físico geográfico e não acabará com a soberania dos Estados, mas a difusão de poder no ciberespaço

---

[142] Tais como jornalistas, repórteres, entre outros. WEIMANN, G. – **New Terrorism and New Media.** Wilson Center Common Labs, 2014. p. 2.

[143] "Percebe-se por aqui a vulnerabilidade de tais sistemas face a ataques cibernéticos e que as suas consequências teriam repercussões por toda a sociedade. Por isto, estes sistemas são considerados infraestruturas críticas." BARBOSA – ***Op cit.*** p. 6.

[144] Segundo Natário e Nunes uma infraestrutura é assim considerada como crítica quando a sua eventual disrupção tem o potencial de afetar seriamente a estabilidade social e a própria soberania do Estado. NATÁRIO, Rui; NUNES, Paulo – Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. In **Revista Militar.** N.º 2547 (Abril), 2014. p. 249-286.

[145] Por sua vez, o mesmo decreto-lei define como Infraestrutura Crítica Europeia aquela "situada em território nacional cuja perturbação ou destruição teria um impacto significativo em, pelo menos, mais um EM da UE, sendo o impacto avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infraestruturas".

[146] MOREIRA, João – **O Impacto Do Ciberespaço Como Nova Dimensão Nos Conflitos.** Boletim Ensino. Investigação n.º 13. Lisboa: Instituto Universitário Militar, 2012. p. 28.

[147] "Paradoxalmente, os países mais industrializados e militarmente mais capazes são também os mais dependentes das TIC e, por conseguinte, os mais expostos a consequências de ciberataques. Esta dicotomia tem promovido uma corrida ao ciberarmamento de grande escala e o estabelecimento de relações difusas entre Estados e o cibercrime organizado – este bem mais experiente neste território." GUEDES – ***Op cit.*** p. 191.

coexistirá e complicará, em grande medida, o que significa exercício de poder nestes domínios"[148].

No meio dos imensos atores que interagem o ciberespaço, o ator Estado está presente e cada vez mais este desenha e alinha a sua Estratégia Nacional de Segurança (ENS) com a sua Estratégia Nacional de Cibersegurança (ENCS)[149]. Esta postura deve-se em grande medida ao facto do ciberespaço constituir um novo poder, pese embora esta opinião não seja consensual entre os diversos autores pois há alguns que defendem que o ciberespaço constitui não mais um poder mas antes mais uma forma de poder, como tantos outros que o Estado detém[150].

De igual modo, o ciberespaço consubstancia uma "área de responsabilidade coletiva, o que leva a que se definam muito bem os papéis daqueles que têm responsabilidade de assegurar a sua segurança e proteção"[151].

Assim, deverá ser consignada a cibersegurança às Forças de Segurança (FS) e a ciberdefesa às Forças Armadas (FA), a fim da preservação do ciberespaço que se tem constituído como vital "na reorganização das dinâmicas sociais, económicas e culturais[152], que passaram a justificar-se num patamar global"[153], bem como a potenciar a associação em torno de interesses comuns e a possibilitar a participação anónima ou de múltiplas identidades digitais em redes de interesses diversas.

Outros modos de atuação e de demonstração de poder no ciberespaço "abrangem atos como a inserção de código malicioso para interromper sistemas ou o roubo de propriedade

[148] NYE, Joseph S. – **Cyber Power. Technical Report.** Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. p. 3.
[149] Portugal lançou o seu Conceito Estratégico de Defesa Nacional em 2013, onde já aí houve uma referência à Estratégia Nacional de Cibersegurança. Já em maio de 2015 foi publicada a primeira Estratégia Nacional de Segurança do Ciberespaço. Cfr. KLIMBURG, Alexander et al – **National Cyber Security: Framework Manual.** Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012.
[150] BETZ, David; STEVENS, Timothy – **Cyberspace and the State: Towards a Strategy for Cyberpower.** Routledge: The International Institute for Strategic Studies, 2011.
[151] SANTOS, Lino et al. – Proteção do Ciberespaço: Visão Analítica. In SOARES, C.; TEIXEIRA, A.; JACINTO, C. (eds.) – **Riscos, Segurança e Sustentabilidade.** Lisboa: Edições Salamandra, 2012. ISBN 978-972-689-247-2. p. 163.
[152] "Assim, se, por um lado, este novo *media* altera a forma de atuação, mormente dando poder a atores que doutro modo a ele não acederiam, por outro, propícia, de forma singular, um conjunto de oportunidades no que concerne ao controlo e à vigilância da sociedade." SANTOS, Lino; GUEDES, Armando – Breves Reflexões sobre Poder e Ciberespaço. In **Revista de Direito e Segurança.** Ano III. N.º 6. 2015. (julho/dezembro). ISSN 2182-8687. p. 203.
[153] AMARAL, Sandra – **O Papel dos Serviços de Informações no Combate ao Ciberterrorismo: o Caso Português.** Lisboa: Academia Militar, 2014. Dissertação de Mestrado. Cfr. igualmente JORDAN, Tim; TAYLOR, Paul A. – **Hacktivism and Cyberwars: Rebels with a cause?** New York: Routledge, 2004.

inteletual. No caso de grupos criminosos, o lucro é a finalidade última, ao passo que às intenções dos governos preside o aumento dos seus recursos económicos"[154].

Neste sentido, as previsões de guerra num futuro próximo apontam para que a mesma seja iniciada "com base num ataque cibernético maciço, para desorganizar as capacidades do inimigo"[155].

Esta premissa tem levado ao desenvolvimento de mecanismos de proteção e defesa com o objetivo de garantir a segurança no ciberespaço, com os Estados a reconhecer a importância do "desenvolvimento de políticas e estratégias cooperativas de combate a ataques cibernéticos, materializadas em iniciativas de caráter nacional e internacional"[156].

Neste contexto, e encarando o ciberespaço como um espaço prioritário, Portugal desenvolveu uma política securitária própria, a Estratégia Nacional de Segurança do Ciberespaço (ENSC), "onde se encontram estabelecidos os objetivos e linhas estratégicas que garantem a segurança cibernética em Portugal"[157].

Assim, a Resolução do Conselho de Ministros (RCM) n.º 115/2017, de 24 de agosto, com base na RCM n.º 36/2015, de 12 de junho, veio aprovar a ENSC, com o propósito de aprofundara segurança das redes e da informação e, em especial, garantir a proteção e a defesa das IC e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas[158].

Nos termos desta Resolução veio-se criar um grupo de projeto denominado Conselho Superior de Segurança do Ciberespaço (CSSC), que funciona na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar, e cuja missão consiste em

---

[154] "Tal é o caso da China que tem sido acusada, por vários outros países, de tal procedimento. Provar este tipo de ataques é, frequentemente difícil, uma vez que os atacantes camuflam as suas intrusões através de servidores em outros países, o que dificulta a atribuição de responsabilidades. Ainda nesta linha, não são escassos os relatos de ataques implicados com a guerra, (Iraque em 2003, Geórgia em 2008) ou de sabotagem de equipamentos eletrónicos. Israel terá recorrido a meios cibernéticos para derrotar as defesas aéreas sírias antes de bombardear um reator nuclear secreto." PARAÍSO, Ariana – Da sociedade em rede e do novo espectro de ameaças: o ciberespaço In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 54 Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2017. p. 14.

[155] Afirmação de António Guterres, atual Secretário-Geral da ONU. ALMEIDA, Cláudia – A Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço. In **III Seminário IDN Jovem.** N.º 30. Lisboa: IDN, [s.d.]. p. 271.

[156] *Ibidem*.

[157] FREIRE, Fernando; NUNES, Paulo – Estratégia da Informação e Segurança no Ciberespaço. In **Estratégia da Informação e Segurança no Ciberespaço**. 2013. Vol. 12. Lisboa: Instituto de Defesa Nacional, IDN Cadernos. ISBN: 978-972-27-2272-8. p. 9-94.

[158] A responsabilidade pela segurança do ciberespaço nacional encontra-se distribuída por diferentes entidades com missões e objetivos diversos, sendo, por essa razão, imperioso assegurar a existência de uma abordagem transversal e integradora das variadas sensibilidades, necessidades e capacidades dos diversos setores com intervenção neste âmbito. Resolução do Conselho de Ministros n.º 115/2017. **Diário da República I Série.** N.º 163 (24-08-2017). p. 5037.

assegurar a coordenação político-estratégica para a segurança do ciberespaço e o controlo da execução da ENSC e da respetiva revisão[159]. Além disso, reforçou-se o dever de notificação de incidentes[160] de cibersegurança por parte de entidades públicas e dos operadores de infraestruturas críticas, com vista a assegurar a eficácia da respetiva coordenação operacional, bem como uma melhor avaliação situacional, tal como já previsto na alínea e) do n.º 2 do acima referido Eixo 1 da ENSC.[161]

Em complemento, verificamos a necessidade de existir no ciberespaço uma "cooperação internacional mais intensa e eficaz, que promovesse uma ação multi ou transnacional conjunta, que fizesse face ao crescendo de ameaças no ciberespaço"[162].

Voltando à ENSC, saliente-se que a mesma foi elaborada com o objetivo de preparar o Estado Português e as suas respetivas instituições para os novos desafios promovidos pela evolução tecnológica e pela crescente dependência das tecnologias da informação na prossecução das tarefas que asseguram o normal funcionamento do Estado.

A ENSC possui quatro objetivos estratégicos[163], a saber: (1) a promoção de uma utilização consciente, livre, segura e eficiente dos meios informáticos; (2) a proteção dos direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos indivíduos nacionais; (3) o fortalecimento e a garantia de segurança no ciberespaço, das infraestruturas críticas e dos serviços nacionais vitais; e (4) a afirmação do ciberespaço como um domínio de desenvolvimento económico e de inovação.

Deste modo, a estratégia definida pela RCM n.º36/2015 assenta em seis eixos, associados: à estrutura e segurança no ciberespaço e à coordenação político-estratégica; à coordenação das restantes organizações nacionais através do Centro Nacional de Cibersegurança (CNCS), ao desenvolvimento da capacidade de defesa cibernética e de resposta a incidentes, sobretudo através do *Computer Security Incident Response Team* (CSIRT); ao

---

[159] O CSSC tem como objetivos: a) Assegurar a coordenação político-estratégica para a segurança do ciberespaço; b) Verificar a implementação da ENSC; c) Propor a revisão e elaborar a ENSC; d) Pronunciar-se sobre a ENSC previamente à sua submissão para aprovação; e) Elaborar anualmente, ou sempre que necessário, relatório de avaliação da execução da ENSC; f) Propor ao Primeiro-Ministro, ou ao membro do Governo em quem aquele delegar, a aprovação de decisões de caráter programático relacionadas com a definição e execução da ENSC; g) Responder a solicitações por parte do Primeiro-Ministro, ou do membro do Governo em quem aquele delegar, no âmbito da sua missão.

[160] Determina que as entidades públicas e os operadores de infraestruturas críticas têm o dever de notificar o Gabinete Nacional de Segurança/Centro Nacional de Cibersegurança, sem demora injustificada, dos incidentes com impacto importante na segurança das redes e dos sistemas de informação. Resolução do Conselho de Ministros n.º 115/2017. **Diário da República I Série.** N.º 163 (24-08-2017). p. 5037.

[161] *Ibidem*.

[162] MILITÃO, Octávio – **Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional.** Lisboa: Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa, 2014. Dissertação de Mestrado. p. iv.

[163] Ver Anexo da Resolução do Conselho de Ministros n.º 36/2015.

combate ao crime informático, através da revisão e atualização da legislação nacional (de forma periódica), e do melhoramento das capacidades técnicas e humanas da Polícia Judiciária; à proteção do ciberespaço e das suas infraestruturas, através de uma maior robustez dos sistemas e da informação associada, e de mecanismos de deteção precoce de ameaças; à educação, sensibilização e prevenção e promoção do uso seguro das TIC; e à cooperação entre diferentes atores do panorama nacional e internacional (nomeadamente com CSIRT's, UE e OTAN)"[164].

Com efeito, poderemos então definir a ENSC como "o conjunto de iniciativas integradas (de natureza orgânica, operacional e genética), cujo objetivo é potenciar a livre utilização do ciberespaço e a garantia da sua segurança, promovendo a proteção das informações confidenciais nacionais – a chamada infraestrutura crítica – contra eventuais ataques de piratas informáticos, de âmbito nacional ou internacional que, pelo seu potencial disruptivo afetem a sociedade nacional e a defesa dos interesses nacionais"[165].

Nesta perspetiva, surge o já referido CNCS[166] com o objetivo de dotar as entidades do Estado e os operadores de IC nacionais com ferramentas com capacidade para analisar, mitigar e proceder à resolução de incidentes securitários no ciberespaço.

A principal missão do CNCS[167]é a de contribuir para que "em Portugal se faça um uso livre, confiável e seguro, através da promoção de contínuas melhorias da cibersegurança nacional e da cooperação internacional, em articulação com todas as entidades competentes, assim como da implementação das medidas e instrumentos necessários à antecipação, deteção, reação ou recuperação em caso de iminência ou ocorrência de incidentes ou ciberataques que ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais"[168].

---

[164] ALMEIDA – ***Op cit***. [s.d.]. p. 279.
[165] ALMEIDA – ***Op cit***. [s.d.]. p. 280.
[166] O estabelecimento dos termos de funcionamento do Centro Nacional de Cibersegurança foi previsto no Decreto-Lei n.º 69/2014. **Diário da República I Série.** N.º 89 (09-05-2014). p. 2712-2719.
[167] "De modo a prosseguir a sua missão, o CNCS possui diversas competências, que aqui apresentamos: (1) Desenvolver as capacidades nacionais de prevenção, monotorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de defesa do ciberespaço e ciberataques; (2) Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de cultura nacional de cibersegurança; (3) Exercer autoridade nacional em termos de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais; (4) Contribuir para assegurar a segurança e defesa dos sistemas de informação e comunicação do Estado português e das suas infraestruturas críticas; (5) Promover e assegurar a articulação e cooperação entre os vários intervenientes e responsáveis nacionais no âmbito da cibersegurança; (6) Apoiar o desenvolvimento de capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da segurança informática; (7) Coordenar a cooperação internacional em matérias de cibersegurança em pareceria com o Ministério dos Negócios Estrangeiros; (8) Entre outras competências." ALMEIDA – ***Op cit***. [s.d.]. p. 281.
[168] ALMEIDA – ***Op cit***. [s.d.]. p. 280.

Por outro lado, a Lei n.º 46/2018[169], de 13 de agosto, estabeleceu o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do PE e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

Nos termos deste normativo legal, o seu art.º 4.º (ENSC) veio definir o enquadramento, os objetivos e as linhas de ação do Estado nesta matéria, de acordo com o interesse nacional (n.º 1), sendo esta Estratégia aprovada por Resolução do Conselho de Ministros, sob proposta do Primeiro-Ministro, ouvido o CSSC[170] (n.º 2).

No art.º 6.º vêm definidas as competências do CSSC: a) assegurar a coordenação político-estratégica para a segurança do ciberespaço; b) verificar a implementação da ENSC; c) pronunciar-se sobre a ENSC previamente à sua submissão para aprovação; d) elaborar anualmente, ou sempre que necessário, relatório de avaliação da execução da ENSC; e) propor ao Primeiro-Ministro, ou ao membro do Governo em quem este delegar, a aprovação de decisões de carácter programático relacionadas com a definição e execução da ENSC; f) emitir parecer sobre matérias relativas à segurança do ciberespaço; g) responder a solicitações por parte do Primeiro-Ministro, ou do membro do Governo em quem este delegar, no âmbito das suas competências.[171]

Já o art.º 7.º vem concretizar a dependência do CNCS[172]no Gabinete Nacional de Segurança, bem como designar o primeiro como a Autoridade Nacional de Cibersegurança. Nos termos do n.º 2 deste artigo, o CNCS tem por missão garantir que o País usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento da Administração Pública (AP), dos operadores de IC, dos operadores de serviços essenciais e dos prestadores de serviços digitais[173]. O n.º3 do mesmo artigo vem definir o CNCS como o ponto de contacto único nacional para efeitos de cooperação internacional,

[169] Lei N.º 46/2018. **Diário da República I Série.** N.º 155 (13-08-2018). p. 4031-4037.
[170] Lei N.º 46/2018. **Diário da República I Série.** N.º 155 (13-08-2018). p. 4032.
[171] Lei N.º 46/2018. **Diário da República I Série.** N.º 155 (13-08-2018). p. 4033.
[172] *Ibidem*.
[173]O CNCS exerce as funções de regulação, regulamentação, supervisão, fiscalização e sancionatórias nos termos das suas competências, bem como tem o poder de emitir instruções de cibersegurança e de definir o nível nacional de alerta de cibersegurança, sendo que qualquer disposição legal de cibersegurança carece do parecer prévio do CNCS (n.ºs 4, 5 e 6 do art.º 7.º).

sem prejuízo das atribuições legais da Polícia Judiciária relativas a cooperação internacional em matéria penal. Por último, o CNCS atua em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, devendo comunicar à autoridade competente, no mais curto prazo, os factos de que tenha conhecimento relativos à preparação e execução de crimes (n.º 7).

O art.º 8.º vem definir que a Equipa de Resposta a Incidentes de Segurança Informática Nacional é o «CERT.PT», o qual funciona no CNCS.[174]

O «CERT.PT» possui as seguintes competências (art.º 9.º): "a) exercer a coordenação operacional na resposta a incidentes, nomeadamente em articulação com as equipas de resposta a incidentes de segurança informática setoriais existentes; b) monitorizar os incidentes com implicações a nível nacional; c) ativar mecanismos de alerta rápido; d) intervir na reação, análise e mitigação de incidentes; e) proceder à análise dinâmica dos riscos; f) assegurar a cooperação com entidades públicas e privadas; g) promover a adoção e a utilização de práticas comuns ou normalizadas; h) participar nos fora nacionais de cooperação de equipas de resposta a incidentes de segurança informática; i) assegurar a representação nacional nos fora internacionais de cooperação de equipas de resposta a incidentes de segurança informática; j) participar em eventos de treino nacionais e internacionais"[175].

No que respeita aos requisitos de segurança para a AP e operadores de IC, de acordo com o art.º 14.º, os mesmos devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, as quais devem garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes (n.ºs 1 e 2)[176].

Por outro lado, abordemos agora o ciberespaço na sua componente mais militar.

Assim, se compararmos o orçamento militar com o custo da vigilância e o custo dos ciberguerreiros, facilmente veremos que os sistemas de armas convencionais custam muito dinheiro, pelo que, podemos afirmar que "os ciberguerreiros ou a vigilância em massa são super baratos em comparação com uma aeronave apenas"[177].

---

[174] Lei N.º 46/2018. **Diário da República I Série.** N.º 155 (13-08-2018). p. 4033.
[175] Lei N.º 46/2018. **Diário da República I Série.** N.º 155 (13-08-2018). p. 4033-4034.
[176] A AP e os operadores de infraestruturas críticas tomam as medidas adequadas para evitar os incidentes que afetem a segurança das redes e dos sistemas de informação utilizados e para reduzir ao mínimo o seu impacto (n.º 3). Lei N.º 46/2018. **Diário da República I Série.** N.º 155 (13-08-2018). p. 4034.
[177] A crescente quantidade de manuais e ferramentas disponíveis na internet tem "permitido que qualquer pessoa, mesmo sem conhecimentos profundos de computação, consiga realizar ataques cibernéticos a diferentes alvos ligados à rede. Estes ataques possibilitam ao invasor ter acesso ao sistema, alterar ou destruir informações importantes de pessoas e organizações, além de obter ganhos financeiros." ASSANGE, Julian – **Cypherpunks. Liberdade e o futuro da internet.** Lisboa: Editempo Editorial, 2013. p. 47.

Para concluir, refira-se que já em 2011, a Casa Branca publicou a Estratégia Internacional para o Ciberespaço, a qual observou que "o desenvolvimento de normas para a conduta do Estado no ciberespaço não exige uma reinvenção do direito internacional consuetudinário, nem torna obsoletas as normas internacionais existentes. Normas internacionais de longa data que orientam o comportamento do Estado – em tempos de paz e conflito – também se aplicam no ciberespaço"[178].

1.1.3. A Cibersegurança

> A internet tem vindo a converter-se num novo campo de batalha não convencional cujos rostos invisíveis tendem paulatinamente a dominar o ciberespaço, dotando-se de uma arma que representa uma maior perigosidade e ameaça do que a nuclear num cenário virtual dotado de soldados digitais devidamente preparados para atuar em ambiente de ciberguerra. A arma por excelência no ciberespaço reside na capacidade de enviar códigos que consigam quebrar todo o tipo de protocolos de segurança nas mais diversas redes informáticas. No campo de ação do ciberespaço, a obtenção de informação não representa somente um objetivo concreto, verifica-se assim a constituição de outros, como por exemplo, detetar vulnerabilidades em redes estratégicas para a sobrevivência do Estado.[179]

A segurança no ciberespaço é habitualmente designada como cibersegurança.

A mencionada segurança visa o respeito dos "direitos, liberdades e garantias constitucionalizados nas plataformas digitais"[180], procurando-se conseguir impedir a propagação do nível de ameaças.

A cibersegurança refere-se assim à "segurança da informação digital armazenada nas redes eletrónicas, assim como a segurança das redes que armazenam e transmitem a informação"[181].

A ciberatividade maliciosa tem tido um crescimento exponencial e um aumento da sua sofisticação, o que aliado à "velocidade a que ocorrem os eventos no ciberespaço,

---

[178] Tradução livre do autor. SCHMITT, Michael – International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. In **Harvard International Law Journal.** Vol. 54. Harvard: Harvard College, 2012. p. 13.

[179] MARTINS, M. – Ciberespaço: uma Nova Realidade para a Segurança Internacional. In **Nação e Defesa** – Lisboa: Instituto Da Defesa Nacional, 2012. p. 133.

[180] "A cibersegurança preocupa-se em garantir que terceiros não consigam ler, ou modificar mensagens destinadas a outros recetores. Preocupa-se em evitar que pessoas tentem aceder remotamente a serviços a que não estão autorizadas a usar. Preocupa-se também em arranjar maneiras de verificar se uma mensagem alegadamente das finanças é realmente das finanças e não de uma organização criminosa." TELES, Tiago – **Cibersegurança. Deteção de outliers.** Lisboa: Escola Naval, 2015. Dissertação de Mestrado. p. 18.

[181] A cibersegurança e a segurança da informação referem-se geralmente ao mesmo fim. No entanto, a segurança da informação é usada por organizações e profissionais das tecnologias da informação, enquanto a cibersegurança é geralmente usada em ambientes políticos e quando as questões de segurança da informação são enquadradas como as questões de segurança nacional. FERNANDES – ***Op cit.*** p. 14.

acentuam a necessidade de criar medidas preventivas e reativas, postas em prática pelo Estado, para garantir a realização eficaz de qualquer atividade civil e militar"[182].

O termo cibersegurança surgiu em 1990 para relatar a segurança do ciberespaço, a fim de abranger todo um novo conjunto de ameaças e atores. Tal, derivou do facto de "existir uma elevada interdependência entre o ciberespaço e os restantes espaços físicos e sociais bem como um consequente risco sistémico, [levantando] assim duas perspectivas que são independentes de qual é o objecto e que são: a segurança do ciberespaço, na acepção desta como entidade autónoma, e a segurança da componente "ciber" de um qualquer sistema enquanto segurança do ciberespaço desse sistema"[183].

A cibersegurança consiste na "capacidade de uma rede ou de um sistema informático para resistir, com um dado nível de confiança, a acidentes ou ações maliciosas que comprometam: dados (disponibilidade, autenticidade, integridade e confidencialidade); e, serviços (continuidade e qualidade)"[184].

De igual modo, a cibersegurança tem como objetivo principal, ao nível judicial, o da "dissuasão da prática de crimes pela prevenção e, já no limite, pela condenação concreta do autor do crime"[185], uma vez que "os ciberataques representam atos criminalmente relevantes, passíveis de ação penal, tais como os que são dirigidos contra as pessoas ou contra interesses patrimoniais ou ainda, contra dados e informação"[186].

Tal assenta na premissa de que as ameaças tendem a crescer em número de eventos e de perigosidade, situação que é potenciada pela sua organização em rede.

Em complemento, refira-se que "qualquer indivíduo mal-intencionado, mesmo sem conhecimentos no domínio da informática, pode adquirir *software* "pronto a usar" na *darkweb*, mediante pagamento, ficando em condições de se comportar como um *cracker* experiente"[187].

Porém, o desenvolvimento da era digital conduz à evolução da cibersegurança, o que se traduz na diminuição das vulnerabilidades de *software*. Todavia, a permanente ligação das pessoas à internet aumenta a sua exposição aos riscos e ameaças da mesma.

---

[182] FRIAS, Óscar – **Cyber Intelligence.** A obtenção de Informações a partir de fontes abertas no Ciberespaço. Lisboa: Academia Militar, 2013. Dissertação de Mestrado. p. 18.
[183] RODRIGUES – ***Op cit.*** 2016. p. 8.
[184] CASIMIRO, Sofia – Curso de Mestrado em Guerra de Informação / *Competitive Intelligence* da Academia Militar, do ano letivo 2014-2015. Slide 26.
[185] *Ibidem*.
[186] *Ibidem*.
[187] "O *software* malicioso cresce em quantidade e complexidade, ao passo que o *software* comercial, chamemos-lhe assim, tende a ser feito à pressa, apresentando inúmeras vulnerabilidades, como resultado da enorme competição registada entre empresas do setor, que obriga a uma rápida apresentação de resultados e a uma redução dos custos de produção dos produtos a disponibilizar." RODRIGUES – ***Op cit.*** 2016. p. 13-14.

Deste modo, a defesa e segurança do ciberespaço e das redes de comunicação assume-se atualmente como uma das grandes preocupações dos Estados, pelo que a "cibersegurança passará tanto pela projeção de estratégias que protejam não só os utilizadores, mas também o espaço virtual e físico do ciberespaço, assim como todas as infraestruturas e serviços que dele dependam"[188].

Deste modo, a cibersegurança assume um papel vital para as organizações públicas e privadas, pelo que a adoção de uma segurança eficaz das informações compreende várias camadas de defesa que trabalham juntas para proteger as informações, o acesso a redes e os sistemas de informação[189].

Neste sentido, recordemos que já em 2003, e "no rescaldo dos atentados às Torres Gémeas, na Estratégia Nacional para a Cibersegurança dos Estados Unidos era admitida a forte dependência que estes Estados detinham das redes de comunicação e da internet"[190].

Nos anos subsequentes foram adotadas outras medidas um pouco por todo o mundo, em particular pelos EUA e, sobretudo, pela Europa, em "resposta aos atentados de que foi vitima em Espanha e em Londres, como os ataques cibernéticos ao Governo da Estónia"[191].

Assim, a "utilização indevida e abusiva das potencialidades e vulnerabilidades do ciberespaço quer como meio, quer como fim, para perpetrar ataques contra os Estados e contra as sociedades, tem exigido uma cada vez mais refinada estratégia de combate às ameaças ao ciberespaço"[192], não obstante a dificuldade da sua aplicação, devido às características inerentes ao próprio funcionamento do ciberespaço.

Neste sentido, os EUA fizeram refletir na sua doutrina militar o aumento significativo do uso dos sistemas de informação para o apoio das operações militares, o qual se refle-

---

[188] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** e MANUEL, A. – **A dimensão política da Segurança para o Ciberespaço na UE**. Açores: Universidade dos Açores, 2014. e BARBOSA– ***Op cit.*** p. 12.

[189] A premissa é que, se uma camada falhar, outras também falharão. Camadas técnicas, como *firewalls*, *patches* de *software*, sistemas de deteção de intrusão, programas antivírus e criptografia são geralmente as únicas áreas consideradas em segurança cibernética. No entanto, ataques de penetração eficazes geralmente são sociais, e não técnicos, e são responsáveis pela maioria dos ataques cibernéticos. De facto, a vulnerabilidade mais significativa na segurança da informação está relacionada com o erro humano. Tradução livre do autor. DEFENCE – ***Op cit.*** p. 190.

[190] Admitindo a vulnerabilidade das infraestruturas críticas e das consequências que possíveis ataques poderiam ter no seu funcionamento (das infraestruturas e do próprio Estado), foi delineada uma estratégia que priorizou não só questões de ação e resposta como de prevenção e educação, numa tentativa de combate à ameaça.THE WHITE HOUSE – **Secure Cyberspace.** GOV US Executive Branch, 2003. p. 2-4.

[191] BARBOSA – ***Op cit.*** p. 13.

[192] A utilização da internet pressupõe uma certa liberdade da qual os seus utilizadores não pretendem abdicar, pois é esta liberdade que torna a internet tão atrativa. Ora, como vemos, são as próprias vantagens do ciberespaço que se materializam nas suas vulnerabilidades e estes princípios de livre utilização e circulação na internet são, por conseguinte, os que a tornam ainda mais perigosa e de difícil controlo.LIN, H. S. et al – **Toward a safer and more secure cyberspace.** 2007. e BARBOSA – ***Op cit.*** p. 13.

tiu na dimensão do ciberespaço como campo de batalha[193]. Tal, levou a definir ciberespaço no dicionário de termos militares, como "um domínio global dentro do ambiente de informação consistindo em redes inter-dependentes de infraestruturas de tecnologia da informação, incluindo a internet, redes de telecomunicações, sistemas de computadores, integrando processadores e controladores"[194].

Deste modo, refiram-se a título de exemplo, as directivas NSPD-5410/HSPD-2311, de 8 de Janeiro de 2008 e 5 de Junho de 2008, respetivamente, da administração George W. Bush, as quais se referem ao ciberespaço como sendo o "conjunto de "redes inter-dependentes de infra-estruturas de tecnologia da informação, incluindo a internet, redes de telecomunicações, sistemas de computadores, integrando processadores e controladores em indústrias críticas. O uso comum do termo também se refere ao ambiente virtual de informação e interações entre pessoas"[195].

Já no Reino Unido, de acordo com a estratégia de cibersegurança do centro de operações de cibersegurança, o ciberespaço "engloba todas as formas de rede, atividades digitais; este inclui o conteúdo e as ações conduzidas através das redes digitais"[196].

Por outro lado, a França refere-se ao ciberespaço, no Livro Branco de Defesa e Segurança Nacional, como um "novo campo de ação, dentro do qual já se desenrolam operações militares, constituído por uma série de redes, diferentes do espaço físico, sem fronteiras, evolutivo, anónimo e onde a identificação de um agressor é muito delicado"[197]. De igual modo, encontramos uma outra definição possível para este novo domínio no dicionário de referência da língua francesa Petit Robert, o qual prescreve o ciberespaço como o "espaço de comunicações criado pela interconexão mundial de computadores"[198].

Por último, e citando um autor nacional, apresenta-se uma definição de ciberespaço do General Loureiro dos Santos, que define este espaço como sendo "o espaço virtual, gerado pelos elementos tecnológicos dos computadores, toda essa área da informática, onde se efetuam interações entre as pessoas, organizações, entre países, de toda a natureza, interações económicas, sociais, políticas, espaço virtual, sustentado, apoiado, gerado por

---

[193] JP 2-01.3. – **Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace.** 2000.
[194] JP 1-02. – **Department of Defense Dictionary of Military and Associated Terms.** 2009. p. 139.
[195] CASA BRANCA – **Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.** Washington: [s.n.], 2009. p. 1.
[196] OCS – **Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space.** Norwich: TSO, 2009. p. 7.
[197] DÉFENSE ET SÉCURITÉ NATIONALE – **Le Livre Blanc.** Paris: Odile Jacob, 2008. p. 53.
[198] ROBERT, Petit – **Le nouveau Petit Robert de la Langue Française 2010.** [Em Linha]. [Consult. 05 Mai. 2019]. Disponível em WWW:<URL: http://pr2010.bvdep.com/version-1/pr1.asp.

tecnologia que nos permite fazer isso"[199]. A título de exemplo, indica-se uma lista de setores, tais como, energia, informação, comunicações e tecnologias, água, alimentação, saúde, economia, administração pública, jurídico e de segurança, administração civil, transportes, indústria química e nuclear, espaço e investigação e respectivos produtos e serviços, considerados como IC que "podem ser danificadas, destruídas ou perturbadas por atos deliberados de terrorismo, catástrofes naturais, negligência, acidentes, atos de pirataria informática, atividades criminosas e comportamentos mal intencionados"[200].

Desta feita, a Estratégia da UE para a Cibersegurança reporta-se, regra geral, "às precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas ou que as possam danificar"[201], com o objetivo de "manter a disponibilidade e a integridade das redes e infraestruturas e a confidencialidade das informações nelas contidas"[202].

A cibersegurança irá continuar a constituir-se como uma das principais preocupações ao nível mundial, considerando a cada vez maior virtualização da informação e não esquecendo que a informação é poder.

A gestão da cibersegurança através da supervisão centralizada a nível europeu não é viável, uma vez que a manutenção de um bom nível de cibersegurança no contexto da UE envolve diferentes setores com diferentes jurisdições e responsabilidades, tanto a nível nacional como da UE. Neste contexto, "os governos nacionais são os principais responsáveis pela manutenção de um bom nível de segurança e devem cooperar a nível da UE em caso de riscos e falhas de segurança que ultrapassem as fronteiras nacionais"[203]. Assim, a estratégia europeia passa pelo incentivo aos EM para a partilha de informações entre "as estruturas nacionais envolvidas na segurança cibernética e no setor privado, para que pos-

[199] PERES – ***Op cit.*** p. 22.
[200] Por exemplo, distribuição de electricidade, gás e petróleo, internet, controlo da qualidade da água, pagamento de serviços, serviços de emergência, tráfego aéreo, assistência médica e hospitalar, comunicações rádio e navegação, entre outros. LIVRO VERDE – **Livro Verde: Relativo a um programa Europeu de protecção das infraestruturas críticas.** Bruxelas: [s.n.], 2005. COM(2005) 576 final. p. 2.
[201] MACHADO – ***Op cit.*** p. 6.
[202] *Ibidem*.
[203] As estruturas envolvidas na manutenção da segurança cibernética estão organizadas em três áreas fundamentais: segurança de redes e informações (NIS), aplicação da lei e defesa. A nível nacional, os EM deverão ter estruturas nacionais em cada uma das áreas mencionadas.

sam ter uma visão abrangente dos riscos e ameaças à segurança e uma melhor compreensão das técnicas de cibercriminalidade para responder mais rapidamente e efetivamente"[204].

Porém, a UE definiu a sua Estratégia para a Cibersegurança, a fim de almejar um ciberespaço aberto, seguro e protegido. Deste modo, a UE para a concretizar decretou alguns princípios que devem orientar a política de cibersegurança na UE e a nível internacional, a saber: os valores fundamentais da UE aplicam-se tanto no mundo digital como no mundo físico[205], e a necessidade de proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade[206]. Para tal, a Estratégia da UE articula-se em cinco prioridades estratégicas, de acordo com os desafios acima destacados: "garantir a resiliência do ciberespaço[207]; reduzir drasticamente a cibercriminalidade; desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da Política Comum de Segurança e Defesa (PCSD); desenvolver os recursos industriais e tecnológicos para a cibersegurança; estabelecer uma política internacional coerente em matéria de ciberespaço para a UE e promover os valores fundamentais da UE"[208].

Assim, constatou-se a necessidade da adoção de uma legislação rigorosa e eficaz para combater a cibercriminalidade, bem como de formação específica neste campo[209].

Neste sentido, surgiu a Convenção do Conselho da Europa sobre Cibercriminalidade, a designada Convenção de Budapeste, que se assume como "um tratado internacional vinculativo que fornece um quadro apropriado para a adoção de legislação nacional"[210].

---

[204] Tradução livre do autor. AAVV - **Critical Infrastructure Protection: Threats, Attacks and Countermeasures.**Roma: Tenace Editora, 2014 [Em Linha] [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf. p. 8.

[205] "As leis e normas que se aplicam noutros domínios das nossas vidas quotidianas aplicam-se igualmente no domínio do ciberespaço."COMISSÃO EUROPEIA – **Estratégia da UE para a cibersegurança: Um ciberespaço aberto, seguro e protegido.** Bruxelas: JOIN, 2013. p. 4.

[206] "A cibersegurança apenas pode ser sólida e eficaz se se basear nos direitos e liberdades fundamentais consagrados na Carta dos Direitos Fundamentais da UE e nos valores basilares da UE. Reciprocamente, os direitos individuais não podem ser assegurados sem redes e sistemas seguros. Toda a partilha de informações para efeitos da cibersegurança, quando estejam em causa dados pessoais, deve respeitar a legislação da UE sobre proteção de dados e ter plenamente em conta os direitos individuais neste domínio." *Ibidem*.

[207] "A Comissão solicitou à ENISA (Agência da União Europeia para a Segurança das Redes e da Informação) que: preste assistência aos EM no desenvolvimento de capacidades nacionais fortes de resiliência para o ciberespaço, nomeadamente através da formação de especialistas em segurança e resiliência dos sistemas de controlo industriais e das infraestruturas de transporte e de energia; examine a viabilidade da criação de equipas de resposta a incidentes no domínio da segurança informática para os sistemas de controlo industriais para a UE; e continue a apoiar os EM e as instituições da UE na realização regular de exercícios pan-europeus de resposta a incidentes informáticos, que constituirão a base operacional para a participação da UE em exercícios internacionais de resposta a incidentes informáticos. COMISSÃO EUROPEIA – ***Op cit.*** p. 8.

[208] COMISSÃO EUROPEIA – ***Op cit.*** p. 5.

[209] "A Comissão pede à Academia Europeia de Polícia (CEPOL) que, em cooperação com a Europol: coordene a conceção e o planeamento de cursos de formação para dotar os órgãos policiais/judiciais dos conhecimentos e competências especializadas necessários para combater eficazmente a cibercriminalidade." COMISSÃO EUROPEIA – ***Op cit.*** p. 12.

Saliente-se que, a par dos esforços na área da cibersegurança, a UE tem desenvolvido a dimensão da ciberdefesa. Assim, no sentido de aumentar a resiliência dos sistemas de comunicação e informação que apoiam a política de defesa dos Estados Membros (EM) e os interesses da segurança nacional, o desenvolvimento de capacidades de ciberdefesa deve centrar-se na deteção de ameaças informáticas sofisticadas, na resposta a dar e na recuperação posterior[211].

Por outro lado, a UE considera a necessidade do reforço das capacidades em matéria de cibersegurança e desenvolvimento de infraestruturas informáticas resilientes nos países terceiros[212], pelo que "a UE contribuirá para a consecução deste objetivo intensificando os esforços internacionais em curso para reforçar as redes de cooperação entre os governos e o setor privado que visam a proteção das infraestruturas críticas da informação"[213].

De igual modo, a UE apoia em caso de incidente ou ataque informático importante, pelo que se "o incidente parecer estar associado a um crime, a Europol ou o EC3[214] devem ser informados para que – juntamente com as autoridades policiais dos países afetados – possam iniciar uma investigação, preservar as provas, identificar os autores e, em última instância, garantir que sejam alvo de processo judicial"[215].

Com efeito, o tratamento dos ciberincidentes e dos ciberataques "obriga" ao estabelecimento de "redes de contatos e o apoio dos parceiros internacionais, que podem consistir

---

[210] COMISSÃO EUROPEIA – ***Op cit***. p. 10.

[211] "Perante ameaças multifacetadas, há que melhorar as sinergias entre as abordagens civil e militar na proteção dos ativos informáticos críticos. Estes esforços devem ser apoiados pela investigação e desenvolvimento e por uma cooperação mais estreita entre os governos, o setor privado e as universidades da UE. Para evitar duplicações, a UE irá explorar as possibilidades de a UE e a OTAN complementarem os seus esforços para aumentar a resiliência das infraestruturas críticas das Administrações, da defesa e outras infraestruturas informáticas das quais dependem os membros de ambas as organizações." COMISSÃO EUROPEIA – ***Op cit.*** p. 12.

[212] O bom funcionamento das infraestruturas subjacentes que fornecem e facilitam os serviços de comunicações beneficiará de uma cooperação internacional acrescida, que inclua o intercâmbio das melhores práticas, a partilha de informações, exercícios de alerta precoce e de gestão conjunta de incidentes, etc.

[213] COMISSÃO EUROPEIA – ***Op cit.*** p. 18.

[214] EC3 significa *European Cybercrime Centre*. "A EUROPOL criou em 2013 o EC3 para reforçar a resposta da aplicação da lei ao cibercrime na UE e, assim, ajudar a proteger os cidadãos europeus, as empresas e os governos, contra a cibercriminalidade, que custa aos EM da UE, 265 mil milhões de euros todos os anos, sendo o prejuízo para a economia global, de cerca de 900 mil milhões de euros, contabilizando-se unicamente os custos financeiros." COPETO, Rogério – **Cibercriminalidade.** [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://www.lidadornoticias.pt/opiniao-rogerio-copeto-oficial-da-gnr-cibercriminalidade/.

[215] "Se o incidente estiver aparentemente relacionado com espionagem informática ou houver suspeitas de se tratar de um ataque comanditado por um Estado, ou tiver implicações na segurança nacional, as autoridades nacionais de segurança e de defesa alertarão as suas congéneres, para que estas saibam que estão a ser atacadas e se possam defender. Os mecanismos de alerta precoce serão então ativados e, se necessário, também os procedimentos de gestão de crises ou outros. Um incidente ou ataque informático particularmente grave pode constituir razão suficiente para um EM invocar a cláusula de solidariedade da UE (art.º 222.º do Tratado sobre o Funcionamento da UE (TFUE))." COMISSÃO EUROPEIA – ***Op cit.*** p. 21-22.

na atenuação dos efeitos por meios técnicos, na investigação criminal ou na ativação dos mecanismos de resposta e gestão de crises"[216].

No âmbito da gestão de crises, refira-se que são raros os incidentes que atingem os níveis de crise. Porém, os incidentes devem ser tratados como crises potenciais, a fim de não prejudicar a segurança cibernética. Assim, da perspetiva do "planeamento de contingência – especialmente num contexto europeu – a cooperação transnacional e multissetorial é crucial e duplamente importante na gestão de crises cibernéticas"[217].

Nesta perspetiva, surge a necessidade da criação de uma Estratégia Nacional de Cibersegurança, a qual terá como objetivo final a "garantia de informação para que se possam ter todos os detalhes, aquando da criação de um meio seguro para utilização de todos os indivíduos em simultâneo com a garantia de segurança das redes críticas nacionais."[218]

Esta Estratégia tem por base que a "ampla introdução da tecnologia na vida diária da sociedade conseguiu atingir um patamar em que a maioria da população mundial possui um acesso rápido e sem fios à internet"[219].

Por outro lado, importa salientar que existe ainda a "cibersegurança ligada aos serviços informáticos, ou seja, a ciberespionagem[220] e o ciberterrorismo[221],,[222].

Neste contexto, refira-se que a "monitorização de contas ou conversas para efeitos de combate ao ciberterrorismo implica uma forte violação de direitos e garantias de proteção da informação pessoal e privada difíceis de contornar"[223].

---

[216] COMISSÃO EUROPEIA – ***Op cit.*** p. 22.

[217] As ciber crises por natureza não são geograficamente vinculadas ou baseadas em setores, pelo que, a cooperação entre fronteiras e setores se torna uma necessidade absoluta nesse campo. Tradução livre do autor. ENISA – **Report on Cyber Crisis Cooperation and Management.** European Union Agency for Network and Information Security, 2014. ISBN: 978-92-9204-100-7. p. 33.

[218] MILITÃO, Octávio – **Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional.** Lisboa: Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa, 2014. Dissertação de Mestrado. p. 31.

[219] CASTELLS, Manuel – **A Sociedade em rede.** 2ª Ed. São Paulo: UNESP, 1999.

[220] A ciberespionagem é uma variante da espionagem tradicional, é levada a cabo pelos Estados, e tem como foco adquirir conhecimento e recolher informações que possam conceder uma vantagem estratégica sobre terceiros. PEREIRA, Júlio – Cibersegurança – O Papel do Sistema de Informações da República Portuguesa. In **Segurança e Defesa**. Maio-Agosto. Lisboa: Diário de Bordo, 2012.

[221] O ciberterrorismo, para que seja considerado como tal, tem de observar dois critérios cumulativos: o de apresentar uma motivação política e o de desencadear um resultado destrutivo fisicamente visível. NUNES, Paulo – Ciberterrorismo: Aspectos de Segurança. In **Revista Militar.** N.º 2433. Outubro de 2004. [Consult. 15 Mar. 2018]. Disponível em WWW:<URL: https://www.revistamilitar.pt/art.ºpdf/4282.

[222] LEITE – ***Op cit.*** p. 6.

[223] NISSENBAUM, H. – **Where computer security meets national security. Ethics and Information Technology.** 7(2). 2005. p. 61–73.

Esta questão "da segurança do ciberespaço torna-se óbvia quando assumimos que grande parte da informação essencial e sensível dos cidadãos, dos Estados e de outras organizações é partilhada e/ou armazenada na rede"[224].

Com efeito, é necessário mudar o paradigma da segurança cibernética, no sentido de considerarmos os "modelos de justiça criminal e educação social para proteger os elementos altamente distribuídos da rede de informações, estender a administração efetiva da justiça ao crime cibernético e incorporar a consciência e a competência de segurança na engenharia e na prática comum de computadores"[225]. Para tal, é necessária uma abordagem conjunta, pois nenhum grupo isolado de agências consegue combater o cibercrime sozinho.

Deste modo, a abordagem da cibersegurança e da cibercriminalidade deve mudar e expandir-se, assumindo os modelos tradicionais de combate às ameaças internas e transnacional um importante auxílio na segurança cibernética.

Neste patamar, recorde-se que 2017 "foi um ano terrível para a cibersegurança com mais esquemas de *phishing*, *ransomware*, ataques suportados por Estados e novos vetores de ataque", dos quais destacamos "a falha de segurança na Equifax, ataques apoiados por Governos, a manipulação das redes sociais pela Rússia, o *Wannacry*, e incontáveis esquemas de *phishing*".[226] No que respeitou às previsões de cibersegurança para 2018 saliente-se o aumento dos ataques apoiados por Nações e dos ataques através de dispositivos *IoT* comprometidos, bem como o aumento da automação de algumas tarefas de deteção de ameaças, e o facto de a desconfiança ser um dano colateral na guerra ao cibercrime.[227]

Face ao exposto, refira-se que no ciberespaço "podem ser levadas a cabo operações de combate de grande intensidade que visam coagir adversários a ter o comportamento que nos interessa, interceptando, controlando e/ou destruindo os nós onde as redes informáticas se apoiam, ou simplesmente alterando a semântica associada à informação"[228].

---

[224] "Informação, classificada ou não, cuja partilha ou utilização indevida poderá atentar tanto contra direitos e garantias individuais como colocar em risco a segurança e defesa dos próprios Estados." BARBOSA – ***Op cit.*** p. 14.

[225] Tradução livre do autor. LOSAVIO, Michael; SHUTT, J. Eagle; KEELING, Deborah – Changing the game: social and justice models for enhanced cyber security. In SAADAWI, Tarek; JORDAN JR., Louis; BOUDREAU, Vincent – **Cyber Infrastructure Protection.** Volume II. Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 2013. ISBN 1-58487-571-2. p. 85.

[226] COMPUTERWORLD – **Previsões de cibersegurança para 2018.**[Em Linha]. [Consult. 25 Jun. 2018]. Disponível em WWW:<URL: https://www.computerworld.com.pt/2017/12/22/previsoes-de-ciberseguranca-para-2018/#.Wj6cKwdJdmM.email.

[227] *Ibidem*.

[228] SANTOS, José – **As Guerras que já aí estão e as que nos esperam - se os políticos não mudarem.** Mem Martins: Publicações Europa-América, 2009. p. 302.

1.1.4. Os Ciberataques

"*Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks*."[229]
"*A cyber attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11*."[230]

Os ciberataques que ocorreram contra a Estónia e a Geórgia, respetivamente, em 2007 e 2008, tiveram o condão de marcar de forma permanente a sociedade e originaram o despertar das autoridades dos vários Estados para um novo problema derivado da sociedade em rede, o qual se traduz na ameaça da ocorrência de ciberataques e a, quase interdependente, vulnerabilidade da rede e dos sistemas de informação.

Nesta perspetiva, poderemos definir ciberataque como "um ataque lançado geralmente a partir de um computador recorrendo ao método de intrusão e que tem como finalidade adquirir, explorar, perturbar, romper, negar, degradar ou destruir informação constante em computadores ou em redes de computadores, em sistemas e equipamentos eletrónicos ligados a outros equipamentos ou sistemas ou que partilham a mesma estrutura de energia ou o mesmo espaço de emissão eletromagnética, bem como os próprios computadores, rede de computadores, sistema e equipamentos"[231].

Os ciberataques podem desta forma ser considerados como toda a atividade que, aproveitando-se da forte dependência das TIC pelos Estados, empresas e cidadãos, influencia negativamente o seu correto funcionamento[232].

Por outro lado, um ciberataque é um processo complexo, o qual é constituído por diferentes etapas principais. A primeira etapa baseia-se no reconhecimento e correspondente objetivo de identificar as vulnerabilidades no sistema e nas redes. Após o reconhecimento segue-se a intrusão, que se baseia na invasão da rede do adversário. De seguida, surge a inserção de *malware*[233], que consiste na implementação sigilosa do código malicioso. Em

---

[229] Declaração de Jean-Claude Juncker, em 29 de setembro de 2017, na *Tallinn Digital Summit*.
[230] Declaração de Leon Panetta, em 11 de outubro de 2012, Secretário de Estado da Defesa dos EUA. HAÏDAR, Tim – **Cyber 9/11: is the oil & gas industry sleepwalking into a nightmare?** Oil & Gas IQ, 2015. p. 3.
[231] SILVA – ***Op cit.*** p. 29. e MOREIRA, João – **O Impacto Do Ciberespaço Como Nova Dimensão Nos Conflitos.** Boletim Ensino. Investigação n.º 13. Lisboa: Instituto Universitário Militar, 2012. p. 32.
[232] SANTOS, José – **Contributos para uma melhor governação da cibersegurança em Portugal.** Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2011. Dissertação de Mestrado.
[233] "A tendência mais significativa é o uso de *malware* para comprometer os sistemas de controlo de supervisão e aquisição de dados (SCADA). Essa tendência manifestou-se de duas maneiras principais: *malware* disfarçado de aplicativos SCADA válidos e *malware* usado para verificar e identificar protocolos SCADA específicos." Tradução livre do autor. TREND MICRO – Report on Cybersecurity and Critical Infrastructure in the Americas. In **Analysis and Commentary on the State of Cybersecurity in Critical Infrastructure in the Americas.** Organization of American States. p. 8.

último lugar, a "limpeza, que tem como propósito eliminar as provas e os vestígios da existência do ataque"[234].[235]

Recorde-se ainda que o ciberespaço se carateriza por ser "um mundo caraterizado por não possuir fronteiras físicas, que se pretende de livre acesso, sendo um mundo de oportunidades, riscos e ameaças utilizado para veicular e armazenar informação"[236]. Neste sentido, este mundo está a "moldar a sociedade onde vivemos e é aproveitado para, a uma velocidade próxima da luz, transmitir e armazenar conhecimento. Relações sociais, económicas e políticas estabelecem-se entre pessoas, organizações e Estados a uma escala sem precedentes e em todas as vertentes do ciberespaço, com principal ênfase na internet devido à sua globalização"[237].

Historicamente, a deslocação do "Soldado de Bronze"[238] originou o primeiro ciberataque da história, facto que mudou por completo o paradigma da cibersegurança mundial.

A referida deslocação ocorreu num período entre o final da Guerra Fria e o consequente desmembramento da ex-URSS, no qual se verificou um deteriorar das relações entre a Rússia e a Estónia.

Em abril de 2007 um ataque massivo de *Distributed Denial of Service* (*DDoS*)[239] afetou seriamente as infraestruturas de internet do país e provocou o colapso de *websites* pertencentes a organizações como bancos, jornais, entre outros[240].

Este ataque, alegadamente realizado por "*crackers* russos ou estónios de origem russa, também se alastrou aos organismos governamentais, demonstrando com clareza as motivações políticas e étnicas do ataque: a deslocalização do "Soldado de Bronze" do centro da capital estónia para um cemitério militar"[241].

---

[234] SILVA – ***Op cit.*** p. 30.
[235] Tradução livre do autor. TREND MICRO – ***Op cit.*** p. 8.
[236] CUSTÓDIO, Vitor – Uma viagem através do Ciberespaço. In: **Revista A Mensagem.** Lisboa: Regimento de Transmissões, 2016. p. 42-45.
[237] *Ibidem*.
[238] O "Soldado de Bronze" é um monumento em homenagem aos soldados soviéticos mortos na Segunda Guerra Mundial que desde a independência dividiu a população da Estónia, levando a que em 2007 se verificasse a pior crise política internacional de que o país fez parte desde o fim da ex-URSS. LIIK, K. – **The "Bronze Year" of Estonia-Russia relations.** Tallinn: Ministry of Foreign Affairs of Estonia, 2007. [Em Linha]. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: http://vm.ee/sites/default/files/content-editors/web-static/053/ Kadri_Liik.pdf.
[239] *Distributed Denial of Service*, ou seja, ataque distribuído de negação de serviço. JENIK, A. – **Cyberwar in Estonia and the Middle East.**Network Security, 2009.N.º 4. [Em Linha]. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: https://doi.org/10.1016/S1353-4858(09)70037-6. p. 4.
[240] INTERNATIONAL AFFAIRS REVIEW. **Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security**. Washington: George Washington University, 2009.
[241] HERZOG, S. – **Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.** Journal of Strategic Security, 2011. 4(2), p. 49-60.

Este ciberataque às infraestruturas críticas da Estónia foi considerado por muitos como a "primeira ciberguerra na história das relações internacionais e da ciência informática, expondo de forma clara as utilidades das novas tecnologias na promoção de novos tipos de ameaça e os perigos e fragilidades que os Estados enfrentam na era da globalização"[242].

Tais ciberataques levaram outros Estados a refletirem relativamente à possibilidade de ataques cibernéticos levados a cabo por Estados contra outros Estados.[243]

Assim, alguns Estados tomaram medidas para prevenir e mitigar os efeitos de eventuais ciberataques, a saber:

- Os EUA, após o ciberataque ocorrido em 2007 na Estónia, estabeleceram o U.S. *Cyber Command* (USCYBERCOM), o qual planeia, coordena, integra, sincroniza e conduz atividades para: (1) direcionar as operações e a defesa das informações digitais do Departamento de Defesa; (2) conduzir operações militares no ciberespaço em todos os domínios, de forma a garantir a liberdade de ação dos EUA e dos seus aliados no ciberespaço e salvaguardá-lo dos adversários[244].

- No caso do Reino Unido, a solução encontrada passou pela criação em 2011 da UK's *Cyber Security Strategy* (UKCSS), na dependência do *Government Communications Headquarters* (GCHQ), com o intuito de proteger a segurança nacional e salvaguardar os utilizadores da internet. Deste modo, a fim de tornar o ciberespaço no Reino Unido mais seguro, a UKCSS tem como missões[245]: (1) reduzir o risco de ciberataques no Reino Unido; (2) responder efetivamente a incidentes no ciberespaço; (3) entender o ambiente cibernético do Reino Unido, partilhar conhecimentos, reconhecer as vulnerabilidades sistemáticas; (4) garantir a capacidade de cibersegurança do Reino Unido, assumindo a liderança na questão da segurança cibernética no país.

Estes exemplos assumem-se como paradigmáticos da atual importância da cibersegurança, considerando os benefícios da internet, mas acima de tudo do "igual número de oportunidades para ciberterroristas e *crackers*"[246].

---

[242] LESK, M. – **The new front line: Estonia under cyberassault.** IEEE Security & Privacy, 2007. 5(4). [Em Linha]. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: //dx.doi.org/10.1109/MSP.2007.98. p. 76-79.
[243] ALMEIDA – ***Op cit***. [s.d.]. p. 273.
[244] **U. S. Cyber Command.** 2016. [Em Linha]. [Consult. 03 Jan. 2018]. Disponível em WWW:<URL: www.cybercom.mil/About/History/.
[245] YAPP, P. – **The National Cyber Security Centre Incident Management.** London: National Cibersecurity Centre, [s.d.]. [Em Linha]. [Consult. 03 Jan. 2018]. Disponível em WWW:<URL: www.owasp.org/images/1/1e/NCSC_slides.pdf.
[246] "As organizações terroristas e os seus apoiantes, por exemplo, usam frequentemente a internet para tarefas como recolha de informação, recrutamento de novos membros, financiamento, entre outras operações; os *crackers*, por seu turno, utilizam a internet para disseminar diversos tipos de *malware* de forma a obter informação da vítima ou lucros financeiros." ALMEIDA – ***Op cit***. [s.d.]. p. 274.

Neste contexto, a "cibersegurança começou a tornar-se uma prioridade para indivíduos e famílias, assim como para OI's, governos, instituições de ensino e empresas"[247].

Com efeito, não esqueçamos que os Estados são os atores mais importantes do sistema internacional, pelo que será fulcral a análise da sua "importância e a operacionalização das políticas de cibersegurança destes atores das relações internacionais"[248].

1.2. Os Ataques à Estónia em 2007

O ciberataque perpetrado contra a Estónia[249] entre abril e maio de 2007 foi o primeiro grande ciberataque ocorrido contra um Estado, o qual marcou indiscutivelmente o mundo da cibersegurança, tal como já vimos. Contudo, e como usualmente sucede na maioria dos ataques, a atribuição dos mesmos continua a ser um problema por resolver. Porém, neste caso em concreto, suspeita-se que o ataque tenha sido coordenado pela Rússia.

Este caso ocorrido em 2007 na Estónia, a par do ocorrido em 2008 na Geórgia, vieram comprovar que os Estados terão de garantir a utilização segura do ciberespaço aos seus cidadãos, bem como em relação à sua própria soberania. Com efeito, afigura-se como necessário "analisar o risco social e o impacto dos diversos tipos de ciberataques, diferenciando os de motivação criminosa daqueles que, por apresentarem um maior poder disruptivo, possam colocarem risco a Segurança e Defesa do Estado"[250]. Neste sentido, verifica-se a necessidade de identificar a "existência de um nível nacional e supranacional da segurança cibernética, equacionada e integrada em dois domínios diferentes e complementares: a cibersegurança e a ciberdefesa"[251].

---

[247] "Embora a cibersegurança se tenha tornado uma prioridade para toda a sociedade, a sua rápida expansão está a criar e a tornar a cibersegurança mais desafiante, pois não existem soluções permanentes para o problema em questão, dada a sua constante evolução e caraterísticas." GOUTAM, R. – **Importance of Cyber Security.** International Journal of Computer Applications, 2015. 111(7). p. 14-17.

[248] "Deste modo, a liderança dos governos nacionais na criação e implementação de políticas na área da segurança cibernética proporciona uma melhor compreensão e visão do problema, permitindo uma ação nacional coordenada que assegure os objetivos nacionais de segurança no ciberespaço." ITU – **Cybersecurity: The Role and Responsibilities of an Effective Regulator.** Beirut: ICT Applications and Cybersecurity Division, 2009. e ALMEIDA – ***Op cit***. [s.d.]. p. 275.

[249] "A Estónia é um dos países mais pequenos pertencentes à OTAN, contudo, em contrapartida é dos mais desenvolvidos a nível das tecnologias de informação e dependente do ciberespaço". Em 2008, neste país, em cada 100 habitantes existiam 57 utilizadores ligados à internet, muitos dos serviços podiam ser executados via internet, foi dos primeiros países a proporcionar aos seus habitantes participar nas eleições via internet, 97% das empresas já tinham acesso à internet, mais de 97% das transações bancárias eram feitas via internet, mais de 10% das faturas eram electrónicas, o pagamento e identificação podia ser feita a partir do telefone, declarar impostos, todo o Governo já estava ligado em rede, e quase 100% das transações podiam ser executadas utilizando a internet. TIKK, Eneken – **Cyber Attacks Against Georgia: Legal Lessons Identified.** Tallinn: NATO, 2008. PERES, Remi – **A guerra no Ciberespaço: princípios da guerra clássica aplicados na Ciberguerra.** Lisboa: Academia Militar, 2010. Dissertação de Mestrado. p. 33.

[250] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** p. 8.

[251] *Ibidem*.

Com efeito, iremos explicitar as diversas fases e subfases dos ciberataques ocorridos na Estónia para depois evoluirmos para a caraterização, necessariamente breve, dos ataques em si mesmo. De igual modo, abordaremos os alvos dos atacantes, os métodos de ataque utilizados, a origem dos ciberataques e os respetivos impactos.

1.2.1. Caraterização dos Ciberataques e respetivos impactos

1.2.1.1. O evento

Os ciberataques perpetrados contra a Estónia ocorreram entre abril e maio de 2007, sendo possível, contudo, identificar claramente duas fases distintas, a saber: uma primeira que decorreu entre 27 e 29 de abril e onde se assistiram a ataques relativamente simples e sem grande coordenação entre eles; e uma segunda fase que se deu entre 30 de abril e 18 de maio, essa sim, bastante mais sofisticada e onde claramente houve uma coordenação entre os diversos ciberataques. Dentro desta segunda fase podemos ainda subdividi-la em quatro momentos distintos: o primeiro ocorrido em 4 de maio, o segundo em 9 de maio, o terceiro em 15 de maio e o último em 18 de maio de 2007[252].

Após uma sequência de ciberataques contra os sistemas informáticos do Governo da Estónia, a OTAN e os EUA mandaram especialistas em cibersegurança para auxiliar este Estado a recuperar dos referidos ataques, apurar as fontes desses ataques e analisar os métodos utilizados[253].

Por outro lado, este incidente cibernético gerou uma certa controvérsia, considerando a dificuldade no apuramento das responsabilidades dos ataques, bem como a sua classificação em ser: um mero crime, ou seja, cibercrime; ciberterrorismo; ou ciberguerra[254].

O facto de a Estónia ser um dos países particularmente desenvolvidos ao nível das tecnologias de informação, levou a que estivesse mais vulnerável a ataques a infraestruturas críticas da internet e, logo, alvo de ciberataques.

Este conflito foi despoletado pela remoção de uma estátua de bronze situada na capital da Estónia (Tallinn) com destino ao cemitério militar, situação que promoveu diferentes ideologias na Estónia[255].

---

[252] Para um maior aprofundamento do tema recomenda-se a consulta de TIKK, Eneken et al – **International Cyber Incidents.** Tallinn: CCDCOE, 2010.

[253] CLAY, Wilson – **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.** Washington DC: CRS Report for Congress, 2008.

[254] Neste caso, não é possível tirar ilações precisas sobre que tipo de conflito se trata, ou seja, se estamos a falar de um caso de ciberguerra. Porém, a 6 de março de 2009 surgiram revelações do "deputado Russo (Sergei Markov), de que os ataques teriam sido incentivados e coordenados por um dos seus assistentes do qual não podia revelar a sua identidade, e portanto este é um evento que temos de ter em conta como possível modelo de ciberguerra." PERES – ***Op cit.*** p. 32.

Como tal, em 27 de abril de 2007 o país "viveu o que muitos consideram como a primeira guerra no ciberespaço. Uma ofensiva foi lançada contra a Estónia, com o objetivo de bloquear sítios oficiais como por exemplo do Primeiro-Ministro, Parlamento, da Presidência da República, destabilizar as operações dos maiores bancos da Estónia, serviços de saúde e tecnologia, e afetaram os sítios de vários jornais diários"[256].

Porém, o início deste conflito ocorreu em 15 de fevereiro de 2007, após o Parlamento Estoniano ter aprovado a lei para desmantelar a estátua do Soldado de Bronze num prazo de 30 dias, a qual estava situada na capital e tinha sido construída há mais de 50anos.

Depois da aprovação da lei no Parlamento, faltaria apenas a assinatura do Presidente da República da Estónia para avançar com o desmantelamento da estátua, tendo sido neste momento que vários países alertaram a Estónia para a possibilidade de uma eventual retaliação por parte da Rússia, aconselhando a Estónia a não semear atos de discórdia e a criar problemas desnecessários. Todavia, a Estónia acabou por ignorar os pedidos e seguiu com o desmantelamento do Soldado de Bronze a 26 de abril de 2007.

Consumada a tomada de decisão e a correspondente remoção da estátua do seu local habitual, a população estoniana de descendência Russa saiu à rua organizando protestos e vandalizando diversas lojas.

Contudo, e mais gravosa ainda, foi a outra forma de protesto mais silenciosa que foi desencadeada por *hackers* e que teve início a 27 de abril de 2007, a qual acabou por provocar danos enormes na economia[257].

Os ataques cibernéticos fizeram-se sentir num período de 1 mês (27 de abril a 18 de maio de 2007) e foram conduzidos em cinco fases, como forma de protesto com o objetivo de paralisar a economia da Estónia e impedir que a disseminação de informação se fizesse para o exterior. Cronologicamente, os ciberataques ocorreram da seguinte forma[258]:

- Numa primeira fase (27 de abril a 30 de abril) fizeram-se sentir pequenos ataques *DoS*[259], envio de correio electrónico com *spam*, servidores e portais de informação ficaram *offline*,

---

[255] Para os estonianos a estátua, era considerada símbolo de terror, opressão e lembrava um passado mau (período entre 1949-1959) que marcou o início da ocupação ilegal por parte dos soviéticos e de um regime de terror que executou certa de 19.000 estonianos. Para a população Russa que representa cerca de 25% da população residente na Estónia, a estátua do soldado de bronze representava e assinalava o triunfo soviético sobre as tropas nazis. PERES – ***Op cit.*** p. 33.

[256] TVNET – **A guerra no ciberespaço.** 2009. [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://tvnet.sapo.pt/noticias/video_detalhes.php?id=44111.

[257] TIKK – ***Op cit.***

[258] PERES – ***Op cit.*** p. 34.

[259] *Denial of Service*, isto é, ataque de negação de serviço.

sítios ficaram sobrecarregados 400 vezes mais que o normal com excesso de visitas resultando que muitos deles ficassem *offline* no início do conflito.

- Numa segunda fase (4 de maio) deu-se o primeiro ataque *DDoS* em grande escala.
- Numa terceira fase (9 de maio a 11 de maio) verificaram-se ataques ao maior banco da Estónia (*Hansapank*) que ficou *offline* cerca de hora e meia e, novamente, outro ataque *DDoS* em grande escala.
- Numa quarta fase (15 de maio) foram efectuados ataques ao segundo maior banco da Estónia (*SEB bank*) que acabou por ficar *offline* durante cerca de uma hora.
- Numa quinta fase (18 de maio) deu-se o último ataque *DDoS*.

1.2.1.2. Alvos principais dos atacantes

Se o objetivo dos ciberataques tinha subjacentes questões políticas, e se a Estónia era reconhecida por ser uma referência ao nível do *e-gov*, era expetável que as vulnerabilidades viessem a ser exploradas nomeadamente pelos atacantes atingindo alvos políticos. E foi precisamente isso que se verificou e, não obstante, na primeira fase os ataques terem utilizado métodos relativamente simples e terem sido realizados de uma forma pouco coordenada, já durante a mesma eles tiveram impacto na Estónia, ou seja, não foi necessário ocorrer a segunda fase para os efeitos se fazerem sentir.

Os alvos dos atacantes podem ser integrados em quatro categorias. Os primeiros alvos foram políticos e governamentais, como não poderia deixar de ser pelas razões já acima apontadas e que foram as causas que despoletaram estes ataques. Os segundos alvos foram os servidores das instituições que eram responsáveis pela infraestrutura da internet na Estónia na medida em que ela é estruturante, como facilmente se depreende. Os terceiros alvos foram os fornecedores de serviços do setor privado, nomeadamente a banca, não só pelo seu grau de exposição mas também porque a disrupção do seu serviço tinha impacto na vida diária dos cidadãos da Estónia, bem como as agências de notícias. Os quartos e últimos alvos dos ciberataques foram pessoas e outros alvos aleatórios[260].

Assim, no caso da Estónia, os alvos dos atacantes foram os servidores que suportam a infraestrutura da internet na Estónia; o Governo e outras instituições públicas; e os serviços vitais do setor privado, tais como, bancos e agências de notícias.[261]

---

[260] PERES – ***Op cit.*** p. 34.

[261] Curso de Mestrado em Guerra de Informação / *Competitive Intelligence* da Academia Militar, do ano letivo 2014-2015.

1.2.1.3. Métodos de ataque utilizados

Os quatro métodos de ataque utilizados na Estónia foram os seguintes: negação de serviço (*DoS* e *DDoS*), ataques de configuração de *sites* (*website defacement*), ataque a servidores de sistemas de nomes de domínio, e envio massivo de mensagens de correio eletrónico malicioso (*spam*)[262].

O ataque *Denial of Service* (*DoS*), também conhecido como "ataque de negação de serviços" é um método de ataque caraterizado pela tentativa de sobrecarregar um computador ou servidor, de modo a provocar instabilidade ou mesmo impedir a execução das tarefas. Para tal, o *hacker* ou *cracker*, envia tantos pedidos que o computador alvo não os consegue processar e o sistema acaba por ficar sobrecarregado ao ponto de negar o serviço ao utilizador legítimo[263].

O *Distributed Denial of Service Attack* (ataque *DDoS*) é um ataque muito conhecido no âmbito da segurança de redes e que tem tido um grande crescimento em número, velocidade, complexidade e frequência nos últimos anos, que visa afetar a disponibilidade de serviço e a integridade de dados.

Embora este tipo de ataque se enquadre no crime de sabotagem informática, não deixa de ser uma realidade constante nas atividades que estejam conetadas à *web*, quer seja uma empresa *e-commerce*, organizações ou mesmo departamentos governamentais, é apenas uma questão de tempo até sofrerem de um ataque *DDoS.*

Os ataques *DDoS* são um tipo de ataque *DoS*, no entanto, diferem por não serem baseados no uso de um único dispositivo para iniciar o ataque, mas em centenas ou milhares de dispositivos desprotegidos e ligados à internet que executam coordenadamente o ataque (são as denominadas *botnets*). Este tipo de ataque é mais difícil de defender e consegue ter mais sucesso contra alvos maiores e mais rápidos.

Os ataques de configuração de sites, ou também designados por *website defacement*, consistem em modificar ou danificar a aparência de um *site*, outdoor, entre outros.

Em relação aos ataques a servidores de sistemas de nome do domínio e envio massivo de mensagens de correio malicioso (*spam*), podemos indicar que um bom exemplo deste tipo de ataques prende-se com a realização de um ataque de envio massivo de mensagens de correio eletrónico aos utilizadores de uma rede de dados[264], com o intuito

[262] CALDAS – ***Op cit.***
[263] WU, H.; ZHAO, L. – **Web Security: A White Hat Perspective.** Chapter 13: Application-Layer Denial-of-Service Attacks. 2015. p. 344. e SKOUDIS, Ed. **Counter Hack A Step by Step Guide to Computer Attacks and Effective Defenses.** Prentice Hall: Canada, 2006. Capítulo 9, Phase 3.
[264] Este ataque de envio massivo de mensagens de correio eletrónico designa-se por *flood*.

de não permitir que as mensagens realmente pertinentes cheguem ao seu destino, uma vez que se verifica uma sobrecarga do servidor que não permite a normal entrega dos *emails* importantes para essa organização ou particular.

1.2.1.4. Origem dos Ciberataques

O ponto relativo à origem dos ciberataques e, numa fase posterior, à atribuição dos mesmos é um dos pontos mais críticos quando se trata de ataques cometidos no ciberespaço[265]. Todavia, têm sido dados passos importantes neste sentido, nomeadamente, na sensibilização que se tem feito junto das organizações relativa à importância de se salvaguardar a prova[266] para que a análise forense possa ser levada a cabo[267].

Não obstante, até hoje, não ter sido possível atribuir os ciberataques à Rússia, verificou-se que a origem dos mesmos deu-se fundamentalmente a partir de fora da Estónia, tendo sido localizados computadores em 178 países no total, sendo que na primeira fase existiram também ataques realizados por nacionalistas ou indivíduos com motivações políticas que seguindo as instruções fornecidas em russo em diversos fora na internet e *sites*, eles próprios realizavam os ciberataques[268]. Importa ainda relembrar que, na primeira fase, os ataques foram simples e descoordenados entre si, ao invés da segunda onde tudo mudou não só do ponto de vista da sofisticação dos ciberataques, mas também da sua coordenação, o que levou a que o processo de rastreabilidade da origem se tivesse tornado mais difícil de levar avante. Parece, contudo, haver poucas dúvidas que este ataque foi coordenado pela Rússia, sendo que a reforçar este sentimento está o facto de esse país ter-se sempre recusado a colaborar nas investigações posteriores aos ciberataques, mais propriamente na análise forense dos mesmos.

1.2.1.5. Impacto dos Ciberataques

No caso dos ciberataques da Estónia, os impactos fizeram-se sentir a vários níveis.

---

[265] Um artigo que ajuda a desmistificar o problema da atribuição é o **Attributing Cyber Attacks**, escrito por Thomas Rid & Ben Buchanana do Department of War Studies, King's College London, 2014. UK Published online: Journal of Strategic Studies.
[266] Em algumas ainda num estado mais incipiente começarem a ter mecanismos que lhes permitam ter provas.
[267] Aqui, o trabalho conjunto e cada vez mais bem articulado entre organizações do mesmo país, bem como em termos de cooperação internacional tem sido determinante, não tendo sido o caso da Estónia, uma exceção como veremos mais adiante. Um dado interessante que se verificou também no caso dos ciberataques a este país e que revela a crescente eficácia da deteção da origem dos ciberataques é que quando começaram a circular notícias sobre o trabalho de cooperação internacional que estava a ser desenvolvido neste caso concreto, o número de ciberataques começou progressivamente a diminuir.
[268] TIKK – ***Op cit.***

O primeiro, e talvez o que tenha tido uma maior visibilidade, afetou a economia nacional da Estónia, na medida em que setores que assentavam o seu negócio ou operações do dia-a-dia nas comunicações eletrónicas e infraestruturas de ICT[269] foram afetados, como era o caso da banca, empresas ligadas à comunicação social e muitas outras pequenas e médias empresas ligadas ao comércio e dos serviços de *e-gov*.

O segundo nível é indissociável do primeiro, ou seja, os impactos sentidos neste foram uma consequência do que se passou no primeiro, mas agora refletido na vida diária dos cidadãos ao nível da indisponibilidade de informação, meios de comunicação ou ainda no acesso a serviços tão críticos como, por exemplo, levantamento de dinheiro dos bancos.

O terceiro nível de impacto deu-se relativamente ao fluxo de informação com o exterior pois, como facilmente se percebe, este foi prejudicado, ainda que neste contexto tenha sido um mal menor.

Por fim, outro efeito nefasto deste evento ficou a dever-se às consequências que uma das soluções encontradas para conter os ataques gerou e que foi o facto de ter havido um bloqueio do tráfego que vinha do exterior acabando por prejudicar o tráfego legítimo[270].

1.2.1.6. Medidas tomadas para fazer face a Ciberataques

As medidas tomadas concentraram-se fundamentadamente na área técnica e na cooperação internacional, dadas as especificidades do evento, e será sobre estas que nos vamos deter nesta parte, não obstante as medidas de cariz político e legal[271] tomadas.

Um dado interessante e bem revelador da falta de experiência na gestão de crises[272] no ciberespaço foi que num primeiro momento a resposta dada aos ciberataques deu-se individualmente ao nível de cada serviço. Percebendo estes que as suas redes começavam a estar obstruídas e não conseguindo destrinçar o tráfego legítimo do tráfego malicioso, começaram a aligeirar o funcionamento dos seus *sites*, nomeadamente retirando imagens

[269] *Information and Communications Tecnology*.
[270] TIKK – ***Op cit.***
[271] Para mais informação sobre este ponto consultar CALDAS – ***Op Cit.***
[272] Para o General Loureiro dos Santos, o conceito de crise tem a sua génese numa "perturbação no fluir normal das relações entre dois ou mais atores da cena internacional com alta probabilidade do emprego da força". Apresentando-se como "uma sequência de interações" fruto de uma ação concreta que desencadeia ações e reações em forma de respostas a um desafio, dado que "a crise envolve sempre um conflito de interesses que é agudizado por um comportamento de conflito", ela tende a ter o seu "início de forma brusca ou lenta, de intensidade, duração e ritmo variáveis mas que pode evoluir no sentido de uma guerra, no sentido da capitulação de uma das partes ou num entendimento mútuo". VILELA, Carolina – **A Gestão de Crises no Quadro da NATO.** Lisboa: Universidade de Lisboa, Instituto Superior de Ciências Sociais e Políticas, 2013. Dissertação de Mestrado. p. 16.

ou ainda solicitando mais largura de banda aos fornecedores de serviço. Contudo, enquanto a resposta foi individual ela não foi eficaz.

Entretanto, e considerando o evoluir da situação, o Primeiro-ministro da Estónia reuniu o Gabinete de Crises onde juntou, entre outros, representantes do Ministérios das Finanças, Justiça, Interior, Forças de Segurança, fornecedores de serviços de internet, bem como elementos da equipa recém-criada de Resposta a Incidentes de Segurança Informática (CERT-EE) com o objetivo de estancar os ciberataques.

Houve, entretanto, diversas medidas tomadas internamente para alcançar este objetivo, algumas das quais com efeitos nefastos como já vimos acima, sendo de realçar que apenas quando se começou a trabalhar em termos de cooperação internacional aos diversos níveis (operacional, forças de segurança, serviços de *Intelligence* (Intel) e políticos) é que o problema foi sanado. De notar que, em termos operacionais, o controlo das operações ficou sobre a alçada do CERT-EE[273]. Os três CERT nacionais que tiveram um papel determinante neste processo foram o finlandês (o seu contributo destacou-se dos restantes), o alemão e o esloveno. Igualmente decisivo para este desfecho foi a coordenação com os maiores fornecedores de serviços de internet, contando para o efeito com a colaboração de alguns gurus do *internetworking*, entre eles Kurtis Lindqvist, Patrik Faltstrom e Bill Woodcock[274].

Por fim, e para além da cooperação já acima referida, importa destacar a cooperação do ponto de vista das instituições, nomeadamente, a UE e a OTAN, sendo que esta última enviou para a Estónia, juntamente com observadores do US-CERT, entre 8 e 10 de maio, uma equipa com o objetivo de verificarem a situação no terreno e prestarem assistência e aconselhamento.

1.2.2. Enquadramento legal dos Ciberataques perpetrados na Estónia

Neste subcapítulo iremos analisar os ciberataques ocorridos na Estónia à luz do ordenamento jurídico português, os quais utilizaram os já referidos métodos de ataque: negação de serviço (*DoS* e *DDoS*); ataques de configuração de *sites* (*website defacement*); ataques a servidores de sistemas de nome do domínio; e envio massivo de mensagens de correio malicioso (*spam*).

---

[273] SANTOS, Lino – **Contributos para uma melhor governação da cibersegurança em Portugal.** Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2011. Dissertação de Mestrado.
[274] WIRED – **Hackers Take Down the Most Wired Country in Europe.** [Consult. 30 Jun. 2016]. Disponível em WWW:<URL: http://www.wired.com/2007/08/ff-estonia.

1.2.2.1. Ataques *DoS* e *DDoS*

Um ataque de *DDoS*[275] tem como objetivo perturbar o sistema informático, através de entrave, impedimento, interrupção ou perturbação grave de um sistema informático, por qualquer forma de interferência nesse sistema. Este ataque enquadra-se no crime de sabotagem informática, previsto e punido pelo art.º 5.º da Lei do Cibercrime[276] (LC). A pena de prisão poderá ser de 1 a 10 anos na eventualidade de os sistemas afetados darem apoio a uma atividade destinada a assegurar funções críticas essenciais.

Caso estejamos perante um ataque *DDoS* de grandes dimensões, tal como se verificou na Estónia, e considerando a dimensão do ataque, pode colocar-se a possibilidade de se verificar um concurso aparente ou real com o crime de sabotagem previsto no art.º 329.º do Código Penal (CP). Tal terá como fundamento, o facto destes ataques terem resultado na impossibilidade do funcionamento ou desvio dos seus fins normais, de forma definitiva ou temporária, total ou parcialmente, de instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população, infraestruturas de relevante valor para a economia, a segurança ou a defesa nacional, com intenção de destruir, alterar ou subverter o Estado de Direito constitucionalmente estabelecido.

Na eventualidade de estarmos perante o crime de sabotagem previsto no CP, estamos perante um crime público, pelo que a denúncia é obrigatória para as entidades policiais e para os funcionários[277], nos termos do art.º 242.º do Código de Processo Penal (CPP).

Esta denúncia, na forma de participação, é aconselhada sobretudo para possibilitar que a autoridade judiciária inicie, o mais breve possível, as diligências necessárias para obter, regra geral, junto dos prestadores de serviços de comunicações eletrónicas os endereços IP e eventualmente outros dados necessários para identificar os autores dos crimes. Para tais ações é fundamental atuar com o máximo de celeridade possível, procurando assegurar que os prestadores de serviços (ou outras entidades relevantes) ainda estejam na posse desses dados, a fim de cumprir os pressupostos para a preservação dos dados.

Com efeito, o procedimento a adotar nestes casos é a apresentação de uma participação criminal junto do Ministério Público (MP)[278], a fim de permitir as já referidas diligên-

[275] Segundo a CERT, estes ataques são "caraterizados por solicitações em massa direcionados para um *site* ou servidor, fazendo com que ele não suporte as solicitações e fique indisponível, ou seja, impedir que utilizadores legítimos tenham acesso a determinado serviço" PERES – ***Op cit.*** p. 33.
[276] Lei N.º 109/2009. **Diário da República I Série.** N.º 179 (15-09-2009). p. 6319-6325.
[277] Na aceção do art.º 386.º do Código Penal, que consiste essencialmente nos trabalhadores que exerçam funções públicas.

cias através da autoridade judiciária. Neste caso, e considerando a sua relevância para a segurança interna, deveremos informar o CNCS, uma vez que os interesses do Estado poderão ser colocados em causa. Este foi o caso que ocorreu na Estónia, uma vez que os interesses do Estado ficaram em causa, devido a este tipo de atos terem impossibilitado o funcionamento ou desvio dos seus fins normais de instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população.

De acordo com o supracitado, em Portugal poder-se-ia equacionara intervenção do Presidente da República (PR) para que seja declarado o estado de emergência. Nos termos do n.º 2 do art.º 19.º da CRP, o estado de emergência pode ser declarado nos casos de agressão efetiva ou iminente por forças estrangeiras, de grave ameaça ou perturbação da ordem constitucional democrática ou de calamidade pública. O estado de emergência é declarado quando estes pressupostos se revistam de menor gravidade (nomeadamente quando se verifiquem ou ameacem verificar-se casos de calamidade pública, tal como foi o caso em análise) e apenas pode determinar a suspensão de alguns dos direitos, liberdades e garantias suscetíveis de serem suspensos (n.º 3 deste art.º 19.º da CRP e n.º 1 do art.º 9.º da atual redação da Lei n.º 44/86, de 30 de setembro). O PR é a entidade com competência para declarar o estado de sítio ou de emergência, após audição do Governo e com autorização da Assembleia da República (AR).

A declaração do estado de sítio ou do estado de emergência é adequadamente fundamentada e contém a especificação dos direitos, liberdades e garantias cujo exercício fica suspenso, não podendo o estado declarado ter duração superior a quinze dias, ou à duração fixada por lei quando em consequência de declaração de guerra, sem prejuízo de eventuais renovações, com salvaguarda dos mesmos limites (n.º 5 do art.º 19.º da CRP). A declaração do estado de sítio ou do estado de emergência em nenhum caso pode afetar os direitos à vida, à integridade pessoal, à identidade pessoal, à capacidade civil e à cidadania, a não retroatividade da lei criminal, o direito de defesa dos arguidos e a liberdade de consciência e de religião (n.º 6 do art.º 19.º da CRP)[279].

[278] Em qualquer dos casos, deve haver a apresentação de participação criminal junto do Ministério Público (ou junto de autoridades que tenham a obrigação legal de lhe transmitir a participação, tais como, a Policia Judiciária, a Guarda Nacional Republicana ou a Policia de Segurança Pública).

[279] A declaração do estado de sítio ou do estado de emergência confere às autoridades competência para tomarem as providências necessárias e adequadas ao pronto restabelecimento da normalidade constitucional (n.º 8 do art.º 19.º da CRP). A violação do disposto na declaração do estado de sítio ou do estado de emergência ou na Lei n.º 44/86, de 30 de setembro, nomeadamente quanto à execução daquela, faz incorrer os respetivos autores em crime de desobediência (art.º 7.º da atual redação da Lei n.º 44/86, de 30 de setembro).

A execução da declaração do estado de sítio ou do estado de emergência compete ao Governo, que dos respetivos atos manterá informados o PR e a AR (art.º 17.º da atual redação da Lei n.º 44/86, de 30 de setembro).

1.2.2.2. *Website defacement*

O *website defacement* constitui um crime de dano informático, nos termos do art.º 4.º da LC.

Associado a este tipo de crime, podem ocorrer outros, dependendo exatamente do teor das mensagens colocadas no *website* (tais como, difamação, previsto no art.º 180.º do CP, caso ofenda a imagem do PR, ou o incitamento à guerra ou à alteração violenta do Estado de Direito, previsto e punido no art.º 326.º do CP). Este teor poderá igualmente preencher o tipo criminal do crime de ameaça ou mesmo o de terrorismo, à luz da Lei n.º 52/2003, de 22 de agosto[280].

Por outro lado, relacionado com o *website defacement* poderemos estar presentes perante um crime de acesso ilegítimo (art.º 6.º da LC), independentemente da forma da infiltração. Nestes casos, aconselha-se a participação ao MP[281], sendo também conveniente solicitar a intervenção do CNCS e do Centro Nacional de Ciberdefesa, caso se verifique que possa ter impacto na defesa do Estado.

1.2.2.3. Ataques a servidores de sistemas de nome do domínio

No que concerne aos ataques a servidores de sistemas de nome do domínio, um bom exemplo deste tipo de ataques prende-se com a realização de um ataque de envio massivo de mensagens de correio eletrónico aos utilizadores de uma rede de dados (*spam*)[282].

Uma vez que as mensagens enviadas massivamente tinham como objetivo perturbar o funcionamento do correio eletrónico, poderá esta prática enquadrar-se no crime de sabotagem informática (art.º 5.º da LC). Tal assenta no desiderato que se pretende atingir, ou seja, esta situação parece ter como objetivo perturbar o funcionamento do sistema de correio eletrónico para, por exemplo, se verificarem atrasos na receção das mensagens ou, até mesmo, impedir que se vejam as mensagens pertinentes.

Nestes casos, e caso sejam utilizadas *botnets*, dificilmente se conseguirá chegar à verdadeira origem dos ataques, dificultando a responsabilização dos autores do ilícito[283].

---

[280] Alterada pela Lei n.º 60/2015, de 24 de junho.
[281] O procedimento criminal depende de queixa, não sendo obrigatória a apresentação desta queixa.
[282] Este ataque de envio massivo de mensagens de correio eletrónico designa-se por *flood*.

Por outro lado, e dependendo do teor concreto de cada mensagem, poderão ainda verificar-se outros crimes.

1.2.3. Reflexões

Findo este capítulo, importa aqui sumarizar algumas ideias pertinentes que sobressaem do mesmo, das quais se destacam as seguintes:

- Afigura-se necessário conhecer e perceber o contexto em que os países estão inseridos para que seja possível conhecer as ameaças, sendo que, neste caso em concreto, ela estava lá e era possível ser identificada, devido às ações tomadas pelo Governo da Estónia.
- Depois é importante perceber que, quem vai à frente do ponto de vista da inovação, não obstante usufruir de diversos benefícios (por exemplo, vantagens ao nível da eficiência e eficácia dos serviços prestados, mas também ao nível do prestígio que o país granjeava pelo facto de ser uma referência em termos de *e-gov*), tem associada uma maior exposição ao risco de ciberataques. Ou seja, quem trabalha em projetos pilotos ou na área da inovação, sabe que a probabilidade de ocorrem internamente situações não previstas inicialmente ou de outros aproveitarem as vulnerabilidades fundamentalmente associadas à falta de curva de experiência é real, tendo sido este o caso da Estónia.
- Importa pois que, cada vez mais se aposte em áreas como a *Intelligence*, porque na maior parte das vezes a ameaça é passível de ser conhecida previamente a ela se manifestar, devendo existir uma aposta em áreas como a gestão do risco dos ativos críticos. Deste modo, importa apostar igualmente em modelos de ciber resiliência, pois os ciber agentes estarão sempre mais à frente comparativamente com aqueles que trabalham a cibersegurança como apenas mais um processo, por norma, de suporte.
- Por outro lado, importa referir ainda que é fundamental fomentar a cooperação internacional, sem a qual a resposta a este tipo de eventos não é eficaz. Porém, esta não é uma área fácil de trabalho, sendo que no caso do ciberespaço o desafio ainda é maior, a começar pela falta de regras e / ou de aceitação de regras comuns do ponto de vista jurídico que permitam aos países punir quem contra si atuou, não raras vezes com o apoio de outros Estados (fenómeno semelhante ao que se assiste no terrorismo). Para tal, deveremos ter a capacidade de saber aproveitar a experiência já consolidada na área da cooperação internacional contra o terrorismo para evoluirmos na cooperação internacional no âmbito da cibersegurança, nomeadamente na área jurídica, pois esta constitui a coluna vertebral para

[283] Pode ser relevante a participação ao MP para que se consiga desmantelar a *botnet*.

que se possa dar uma resposta cabal aos infratores, em particular, no que respeita à sua responsabilização ao nível criminal, sem prejuízo de eventuais indemnizações pecuniárias pelos danos causados.

- Do ponto de vista mais operacional, deixamos agora aqui algumas orientações para o caso de ocorrer algum ciberataque em Portugal, de acordo com o nosso ordenamento jurídico:

a) Numa vertente internacional dos ciberincidentes, assume particular importância conhecer a origem dos mesmos, podendo estas informações serem recolhidas através das investigações levadas a cabo pelas autoridades judiciárias e órgãos de polícia criminal (OPC's), através das denúncias apresentadas e, de igual modo, da análise do cenário geo-político nacional e internacional, nomeadamente através do Serviço de Informações de Segurança.

b) Afigura-se importante concluir se existem sérios indícios de que os ciberincidentes são instrumentalizados por um Estado identificável ou apenas por alguns grupos isolados ou atores individuais, uma vez que esta informação se considera como vital para perceci-onar se se encontram reunidas as condições para se aplicar o Direito Internacional, caso sejam alcançados certos níveis de impacto no Estado. No caso de não ser possível concluir de forma evidente a atribuição do ciberincidente a um Estado, passaremos a aplicar somen-te o Direito interno, de acordo com a tipologia dos ataques e os respetivos efeitos.

c) De acordo com a alínea anterior, poderemos conseguir atribuir o ciberincidente (como um ataque de *DDoS*) a um Estado quando, por exemplo, esses ciberincidentes ou ciberoperações são originárias de órgãos da sua AP, de entidades mandatadas por esse Estado para exercer funções ou poderes públicos ou de entidades privadas, grupos ou pes-soas singulares que recebam instruções e atuem sob orientação ou controlo desse Estado.

d) Já no caso de se conseguir imputar um ciberincidente a um Estado, o Estado atin-gido pode recorrer a: respostas civis (não militares), nomeadamente à via diplomática; for-ças de segurança interna; tribunais internacionais, a fim de ser aplicado o Direito Penal Internacional; e retaliações, de acordo com o princípio da legalidade.

e) Por outro lado, o recurso a uma resposta militar dependerá da qualificação ou não do ciberincidente, no que respeita ao uso da força. Neste sentido, entende-se que há uso da força quando se verificam estragos físicos ou danos corporais ou, no limite, a morte de pessoas. Com efeito, na prática, será lícito recorrer aos meios militares e ao uso da força apenas quando os ciberincidentes sejam imputáveis a outro Estado e sejam, eles próprios, qualificáveis como uso da força.

f) Nos casos em que não há informações de mortes de pessoas ou danos corporais, poderemos explorar a hipótese de se considerar existir uso da força nas situações em que se verificam danos físicos motivados pela falta de eletricidade e comunicações. Nesta contingência, sendo os ciberincidentes imputáveis a um Estado, de acordo com os indícios recolhidos, e se constate o uso da força, o Estado que é vítima dos ciberincidentes poderá socorrer-se do direito de legítima defesa, nos termos do art.º 51.º da CNU[284].

g) Para que seja efetuado o recurso ao uso da força, no âmbito do direito de legítima defesa, terão de ser respeitados os seguintes princípios pelo Estado, de acordo com o direito consuetudinário internacional: o princípio da necessidade de atuação[285]; o princípio da proporcionalidade na resposta[286]; o princípio da adequação da resposta[287]; e o princípio da atualidade da ameaça[288].

h) Tal como já vimos anteriormente, o Estado vítima caso pretenda fazer o uso da força, mesmo que seja numa situação de legítima defesa, de acordo com o art.º 51.º da CNU, terá de informar o CS das NU[289] e, eventualmente, pedir ajuda militar à OTAN[290]. Neste particular, e tendo já a identificação do ataque por forças estrangeiras identificáveis, o referido Estado deverá informar a OTAN, não só para eventual apoio técnico (nomeadamente, através do CNCS) mas, acima de tudo, para informar os restantes EM quanto ao

---

[284] Em Portugal, caso se concretize a agressão efetiva de forças estrangeiras, o Estado pode recorrer ao uso da força pelas suas Forças Armadas, envolvendo para o efeito o Primeiro-Ministro e o Ministro da Defesa Nacional, bem como o PR na qualidade de Comandante Supremo das Forças Armadas.

[285] As medidas de força adotadas terão como objetivos: obviar a um ataque iminente ou terminar um ataque que está a decorrer. Isto é, terá de se verificar que o recurso a meios pacíficos não será insuficiente para atingir qualquer destes objectivos.

[286] A resposta deverá ser proporcional, ou seja, não deve exceder o necessário para pôr um termo ao ataque. Deste modo, os meios a utilizar devem ser proporcionais/adequados às ameaças identificadas e limitar-se ao necessário para fazer face a essas ameaças.

[287] A resposta terá de ocorrer no momento adequado, ou seja, a mesma deve ocorrer durante um ataque ou quando o mesmo é iminente, para se incluir no direito de legítima defesa.

[288] Para se perceber se o uso da força após a cessação do ataque ainda será legítimo ou se será já retaliação teremos de analisar os seguintes parâmetros avaliativos: (i) a proximidade temporal com o ataque; (ii) o período necessário para identificar o agressor; e (iii) o tempo necessário para preparar a resposta.

[289] Caso o Estado pretenda recorrer ao uso da força ao abrigo de um direito de legítima defesa, deve informar o CS das NU para que não entre em incumprimento com as suas obrigações assumidas na CNU.

[290] Nos termos do art.º 4.º do Tratado do Atlântico Norte, no que respeita à gestão de crises, assegura-se que "as Partes consultar-se-ão sempre que, na opinião de qualquer delas, estiver ameaçada a integridade territorial, a independência política ou a segurança de uma das Partes". Em complemento, e de acordo com o art.º 5.º desse Tratado (Defesa Coletiva) assegura-se que "as Partes concordam em que um ataque armado contra uma ou várias delas na Europa ou na América do Norte será considerado um ataque a todas, e, consequentemente, concordam em que, se um tal ataque armado se verificar, cada uma, no exercício do direito de legítima defesa, individual ou coletiva, reconhecido pelo art.º 51.º da CNU, prestará assistência à Parte ou Partes assim atacadas, praticando sem demora, individualmente e de acordo com as restantes Partes, a ação que considerar necessária, inclusive o emprego da força armada, para restaurar e garantir a segurança na região do Atlântico Norte. Qualquer ataque armado desta natureza e todas mais providências tomadas em consequência desse ataque são imediatamente comunicados ao CS. Essas providências terminarão logo que o CS tiver tomado as medidas necessárias para restaurar e manter a paz e a segurança internacionais".

risco para a sua defesa, a fim de se equacionar um uso conjunto das forças militares de EM da OTAN. Todavia, o exposto, não impede este Estado de adotar as medidas que considere necessárias com as suas próprias FAs.

2. A Cibercriminalidade, o Terrorismo e o Ciberterrorismo

2.1. A Cibercriminadade

Neste subcapítulo iremos fazer um breve enquadramento legal da cibercriminalidade[291], procurando explicitar os principais conteúdos associados a este fenómeno, mas sem a pretensão de fazer uma análise jurídica muito técnica ou aprofundada, explicitando, igualmente, a problemática do cibercrime e da sua investigação.

Atualmente, as ameaças e os principais riscos ligados à criminalidade na Europa estão ligados ao "terrorismo, a graves formas de criminalidade organizada, a cibercriminalidade, (…) ao tráfico de armas e a criminalidade transfronteiriça"[292], os quais se adaptam a uma velocidade extraordinariamente rápida à evolução da ciência e da tecnologia, com o intuito de "se aproveitar ilegalmente e de pôr em causa os valores e a prosperidade das nossas sociedades abertas"[293]. De igual modo, "as ameaças híbridas, a volatilidade económica, as alterações climáticas e a insegurança energética colocam em perigo"[294] a população e o território da UE.

Assim, e tendo por base uma já reiterada prática jurídica nesta área, bem como uma longa e rica reflexão doutrinal, dever-se-ia passar de uma solução inicial avulsa para uma solução mais integrada de conceitos e práticas, que permitisse uma melhor interpretação e que fosse igualmente sistémica, ao invés de se encontrar repartida por diversos diplomas legais, o que nem sempre permite a sua visão completa e de conjunto.

Com efeito, exige-se que seja pensada a conceção e aprovação de uma lei adequada e eficaz, considerando que a criminalidade informática está intimamente ligada à questão dos cidadãos exercerem livremente as suas liberdades e verem os seus direitos respeitados. A proteção das pessoas contra o tratamento de dados pessoais, atendendo à proibição de tratamento de determinados dados pessoais, assim como o direito de acesso aos dados que se

---

[291] Refira-se que a cibercriminalidade pode ser absorvida pelo conceito de terrorismo, nos termos da Lei 52/2003, alterada pela Lei n.º 16/2019, de 14 de fevereiro. Esta situação verifica-se se estivermos perante uma "atuação concertada que vise prejudicar a integridade e a independência nacionais, impedir, alterar ou subverter o funcionamento das instituições do Estado previstas na Constituição, forçar a autoridade pública a praticar um ato, a abster-se de o praticar ou a tolerar que se pratique, ou ainda intimidar certas pessoas, grupos de pessoas ou a população em geral, mediante a prática de crimes contra a vida, integridade física, contra a segurança dos transportes e das comunicações, incluindo as informáticas, telegráficas, telefónicas, de rádio ou de televisão, instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população". Cfr. Aula IV da unidade curricular de Direito da Sociedade de Informação do Mestrado em Guerra de Informação, da Academia Militar, ministrada pela Professora Doutora Sofia Casimiro, ano letivo 2015/16.

[292] UNIÃO EUROPEIA – **Projecto de estratégia da segurança interna da União Europeia: "Rumo a um modelo europeu de segurança".** Bruxelas: Conselho da União Europeia, 2010.

[293] *Ibidem*.

[294] UNIÃO EUROPEIA – **Visão partilhada, ação comum: uma Europa mais forte. Estratégia global para a política externa e de segurança da União Europeia.** 2016. p. 7.

encontrem em registos informáticos, tem dignidade constitucional, o que diz bem da sua importância, através do seu art.º 35º da CRP. Mostrando-se insuficiente esta proteção, apesar de consagrada na lei fundamental, sentiu-se necessidade de transpor estes direitos para leis ordinárias, combinando a evolução tecnológica operada e os direitos dos cidadãos[295].

No que concerne à prevenção da criminalidade e ao combate a ações terroristas que atingem indiscriminadamente populações inocentes, verifica-se a "necessidade de se encontrar um equilíbrio entre o respeito devido ao valor fundamental da privacidade e da proteção dos dados pessoais e o direito igualmente essencial à vida em sociedade que é o da segurança pessoal e dos Estados por via da segurança da informação"[296].

O objetivo passa pelo equilíbrio, considerando "o princípio da proporcionalidade, entre as medidas de segurança da informação que visem impedir as ações criminosas e as ameaças que, por aplicação dessas mesmas medidas, possam atingir a privacidade"[297].

Já a cibercriminalidade pode variar entre "a usurpação de identidade, fraude em cartões de crédito ou fraude bancária em geral, violações várias em propriedade intelectual, violação de privacidade, proliferação de casos de pornografia infantil e abuso de menores, *cyberbullying*, ou, numa vertente mais institucional, ciberataques a instituições e infraestruturas governamentais ou entre empresas privadas (ao nível de espionagem industrial)"[298].

2.1.1. O enquadramento legal da Cibercriminalidade na UE e em Portugal

[295] O CP prevê crimes praticados por meio informático. Contudo, revelando-se extremamente ineficaz e insuficiente para fazer face à evolução informática, surgiu em 1991 a Lei 10/91, de 17 de agosto, a designada Lei da Proteção de Dados Pessoais face à Informática, cumprindo com as garantias já enunciadas na CRP e adaptando a legislação nacional à Convenção 108 do Conselho da Europa relativa à proteção das pessoas sobre o tratamento automatizado de dados pessoais. Esta Lei permitiu contemplar de um modo mais abrangente os crimes informáticos. Torna-se importante realçar que o próprio CP, e por ter sido o primeiro instrumento legislativo a prever esta matéria, tipifica como crime a "Devassa por meio informático", "Violação de correspondência e telecomunicações" e "Burla informática", sendo que a Lei do Cibercrime vem tipificar outros crimes informáticos que serão sumariamente analisados "Falsidade informática", "Dano relativo a programas ou outros dados informáticos", "Sabotagem informática", "Acesso ilegítimo", "Interceção ilegítima" e "Reprodução ilegítima de programa protegido". Cfr. SIMAS – ***Op cit.*** p. 71-75.

[296] VAZ – ***Op cit.*** p. 58.

[297] Os serviços de informações e as FS utilizam a escuta telefónica e a interceção de mensagens para investigar, prevenir ou combater atividades ilícitas como o crime organizado ou o terrorismo. *Ibidem*.

[298] No relatório da Norton, em 2012, estimava-se que os resultados obtidos pelas atividades criminais *online* tivessem ultrapassado os resultados combinados do tráfego de marijuana, cocaína e heroína, apontando-se para valores na casa dos €290 mil milhões. COSTA, João – **Cibercriminalidade. Enquadramento jurídico nacional e europeu** [Em Linha]. Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2012. IX Curso de Mestrado em Direito e Segurança. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://www.academia.edu/10077810/CIBERCRIMINALIDADE_ENQUADRAMENTO_JUR%C3%8DDICO_NACIONAL_E_EUROPEU_Cibercriminalidade_Enquadramento_Jur%C3%ADdico_Nacional_e_Europeu-_IX_CURSO_DE_MESTRADO_EM_DIREITO_E_SEGURAN%C3%87A. p. 8.

A cibercriminalidade assume uma particular preocupação por parte da UE, principalmente, desde os atentados na Estónia, em 2007. Com efeito, a sua visão estratégica para promover a cibersegurança assenta na sua Estratégia de Segurança Interna da União Europeia (ESIUE), a qual está estruturada em cinco prioridades. O reforço dos níveis de segurança para os cidadãos e as empresas no ciberespaço constituiu-se como um desses cinco objetivos estratégicos escolhidos para os anos entre 2010 e 2014[299], o qual pretendeu reduzir drasticamente a cibercriminalidade[300].

Tal, consubstancia-se no facto de, nas últimas duas décadas, a internet ter aumentado o seu papel na sociedade e o inerente impacto em todos os setores da sociedade.Com efeito, "a nossa vida diária, os direitos fundamentais, as interações sociais e as economias dependem do funcionamento fluido das tecnologias de informação e das comunicações"[301].

As "dinâmicas da globalização e da mobilidade humana têm favorecido a capacitação operacional e as operações ilícitas que alavancam a atuação do crime organizado, [pelo que] os serviços de informações têm dado enfoque à prevenção e ao combate contra as redes de facilitação da imigração ilegal, o tráfico de seres humanos, o contrabando, o tráfico de heroína, cocaína, drogas sintéticas e armas de fogo"[302]. Este "esforço tem sido também orientado para a projeção de grupos de criminalidade itinerante e o cibercrime e inclui o acompanhamento aturado da evolução da ameaça associada à pirataria marítima"[303].

Neste sentido, um "ciberespaço aberto e livre tem promovido a inclusão política e social em todo o mundo; derrubou as barreiras entre países, comunidades e cidadãos, permitindo a interação e a partilha de informações e ideias entre todos os pontos do globo; proporcionou um fórum para a liberdade de expressão e o exercício dos direitos fundamentais e deu às pessoas meios para lutarem por sociedades democráticas e mais justas"[304].

---

[299] QUADRADO, António – **A Estratégia de Segurança Interna da UE.** Lisboa: Instituto de Estudos Superiores Militares, 2015. p. 22.

[300] Refira-se que "a cibercriminalidade é uma das formas de criminalidade que mais têm aumentado, fazendo mais de um milhão de vítimas por dia em todo o mundo". FERNANDES – ***Op cit.*** p. 44.

[301] COMISSÃO EUROPEIA – **Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido.** Bruxelas: JOIN, 2013. p. 2.

[302] SISTEMA DE SEGURANÇA INTERNA – **Relatório Anual de Segurança Interna de 2017.** Lisboa: Ministério da Administração Interna, 2018. p. 67.

[303] *Ibidem*.

[304] "Para que o ciberespaço permaneça aberto e livre, devem aplicar-se no universo em linha as mesmas normas, princípios e valores que a UE defende para o mundo físico. Os direitos fundamentais, a democracia e o Estado de direito devem ser protegidos no ciberespaço. A nossa liberdade e prosperidade dependem cada vez mais de uma internet robusta e inovadora, que continuará a prosperar se a inovação por parte do setor privado e da sociedade civil favorecer o seu crescimento. Mas a liberdade em linha exige também segurança e proteção. O ciberespaço deve ser protegido contra incidentes, atividades maliciosas e utilizações abusivas; e os governos têm um importante papel a desempenhar na garantia de um ciberespaço livre e seguro. São várias as funções que competem aos governos: salvaguardar o acesso e a abertura, respeitar e proteger os direitos fun-

Tal, assenta nas TIC e na sua preponderância para o crescimento económico, em todas as suas vertentes, passando a constituírem-se como os seus pilares[305].

Todavia, estes consideráveis benefícios acarretam igualmente vulnerabilidades que afetam o designado mundo digital. Assim, tem-se verificado que "os incidentes de cibersegurança[306], intencionais ou acidentais, estão a aumentar a um ritmo alarmante e poderão perturbar a prestação de serviços essenciais que consideramos garantidos, como a água, os cuidados de saúde, a eletricidade ou os serviços móveis. As ameaças podem ter origens diversas – nomeadamente, ataques criminosos, politicamente motivados, terroristas ou patrocinados por Estados, assim como catástrofes naturais e erros involuntários"[307].

Deste modo, a cibercriminalidade[308] acaba por afetar a economia da UE, sendo esta direcionada contra o setor privado e os particulares, uma vez que os cibercriminosos recorrem a métodos cada vez mais rebuscados para se "introduzirem nos sistemas informáticos, roubarem dados críticos ou exigirem resgates às empresas. O aumento da espionagem económica e de atividades patrocinadas por Estados no ciberespaço coloca os governos e as empresas dos países da UE à mercê de uma nova categoria de ameaças"[309].

Nesta perspetiva, a UE definiu uma intensificação dos seus esforços "nos domínios da defesa, da cibersegurança, da luta antiterrorista, da energia e das comunicações estratégicas, [motivos pelos quais os EM terão de] traduzir em atos os seus compromissos de assistência mútua e solidariedade, consagrados nos Tratados, [no sentido da UE] reforçar o

damentais em linha e manter a fiabilidade e a interoperabilidade da internet. No entanto, o setor privado detém e explora partes significativas do ciberespaço e, por conseguinte, qualquer iniciativa que pretenda ser bem sucedida nesta matéria deve reconhecer o seu papel crucial." COMISSÃO EUROPEIA – ***Op cit.*** p. 2.

[305] As TIC estão atualmente na base dos "complexos sistemas que fazem funcionar as nossas economias em setores fundamentais como as finanças, a saúde, a energia e os transportes; muitos modelos de negócio estão construídos com base na disponibilidade ininterrupta da internet e no bom funcionamento dos sistemas informáticos". *Ibidem*.

[306] "O termo cibersegurança refere-se, geralmente, às precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas ou que as possam danificar. A cibersegurança procura manter a disponibilidade e a integridade das redes e infraestruturas e a confidencialidade das informações nelas contidas." *Ibidem*.

[307] *Ibidem*.

[308] "A cibercriminalidade refere-se, geralmente, a um amplo leque de diferentes atividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais. A cibercriminalidade inclui as infrações tradicionais (por exemplo, fraude, falsificação e roubo de identidade), infrações relativas aos conteúdos (por exemplo, distribuição de material pedopornográfico em linha ou incitamento ao ódio racial) e crimes respeitantes exclusivamente a computadores e sistemas informáticos (por exemplo, ataques contra os sistemas informáticos, recusa de serviço e *software* malicioso)." *Ibidem*.

[309] COMISSÃO EUROPEIA – ***Op cit.*** p. 3.

seu contributo para a segurança coletiva da Europa[310], colaborando estreitamente com os seus parceiros, a começar pela OTAN"[311].

No que diz respeito à cibersegurança, a UE tem como desiderato a almejar a obtenção de um nível elevado de proteção dos seus EM no que se refere a ciberameaças, mas procurando igualmente manter um ciberespaço aberto, livre e seguro. Para conseguir concretizar tal objetivo, será necessário reforçar as "capacidades tecnológicas destinadas a atenuar as ameaças e o aumento da resistência das infraestruturas, redes e serviços críticos, bem como uma diminuição da cibercriminalidade"[312].

Neste sentido, os diferentes atores utilizam a informação de diferentes formas, o que pode ser simultaneamente gerador de novas oportunidades e de novas ameaças no ciberespaço. Tal, terá várias implicações na condução da política e da estratégia dos Estados.[313]

A securização das TIC apresenta desafios de variada ordem. Deste modo, a "combinação entre a quantidade de informação ligada em rede e a crescente complexidade dos sistemas computacionais e das aplicações que a trata tem vindo a tornar estes sistemas e a informação neles contida em alvos extremamente vulneráveis a ataques"[314], pelo que, os

[310]No âmbito da Segurança e Defesa, e "paralelamente à gestão de crises externas e ao reforço de capacidades, a UE deverá igualmente ser capaz de oferecer proteção aos seus membros, a pedido destes, e às suas instituições", nos termos dos seus compromissos de assistência mútua e solidariedade e de forma a concretizar a resposta a "desafios com uma dimensão interna e externa, como o terrorismo, as ameaças híbridas, a cibersegurança, a segurança energética, o crime organizados e a gestão das fronteiras externas". UNIÃO EUROPEIA – ***Op cit.*** 2016. p. 15.

[311] No que respeita à defesa coletiva, a NATO continua a ser o quadro principal para a maioria dos EM. Ao mesmo tempo, as relações UE-NATO não prejudicam a política de segurança e defesa dos membros que não pertencem à NATO. Neste contexto, é necessário reforçar a UE enquanto comunidade de segurança: os esforços europeus de segurança e de defesa deverão permitir à UE atuar autonomamente e contribuir de igual modo para a adoção de medidas, em cooperação com a NATO. UNIÃO EUROPEIA – ***Op cit.*** 2016. p. 7.

[312]Isto significa promover sistemas de TIC inovadores que garantam a disponibilidade e a integridade dos dados, ao mesmo tempo que se garante a segurança dentro do espaço digital europeu através de políticas adequadas sobre o local de armazenagem dos dados e a certificação dos produtos e serviços digitais. UNIÃO EUROPEIA – ***Op cit.*** 2016. p. 16.

[313] GUERRA, Amadeu – Lei de Proteção de Dados Pessoais. In **Estratégia da Informação e Segurança no Ciberespaço**. 2013. Vol. 12. Lisboa: Instituto de Defesa Nacional, IDN Cadernos. ISBN: 978-972-27-2272-8. p. 8.

[314] "No dia 2 de novembro de 1988 a internet foi alvo de um software malicioso do tipo habitualmente designado por *worm*. Este programa informático, criado por Robert Morris com o propósito de se auto-propagar através da rede, foi responsável pela contaminação de mais de 60,000 computadores, afetando negativamente e durante vários dias diversos serviços e a funcionalidade global da internet. A rapidez de propagação e o consequente impacto do designado Morris Worm apanhou a então pequena comunidade da internet desprevenida. Da análise do incidente verificou-se que o que mais prejudicou o normal funcionamento da rede e serviços associados não foi o tempo necessário para encontrar um antídoto eficaz, mas sim a inexistência de uma estrutura organizada que permitisse informar a comunidade da existência do incidente, efetuar uma eficaz distribuição do antídoto e instruir os utilizadores sobre a sua aplicação. Como consequência imediata foi então criado um centro de coordenação de resposta a incidentes de segurança designado de CERT/CC." LOPES, Francisco – **Gestão do Conhecimento – Modelação dos Incidentes e das Respostas.** Lisboa: Universidade Católica Portuguesa, Faculdade de Engenharia, 2010. Dissertação de Mestrado. p. 41-42.

serviços de resposta a incidentes de segurança informática (CSIRTs) têm sido apontados como essenciais na prevenção e reação a este tipo de fenómeno"[315].

Assim, na Estratégia da UE para a Cibersegurança[316]constam, expressamente, os seguintes princípios da cibersegurança: "os valores fundamentais da UE aplicam-se tanto no mundo digital como no mundo físico; proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade; acesso para todos (inclusão digital segura); governação multilateral, democrática e eficiente; uma responsabilidade partilhada para garantir a segurança"[317].

Deste modo, será "necessário integrar de forma horizontal as questões de cibersegurança em todos os domínios de intervenção, reforçando os elementos de cibersegurança nas missões e operações PCSD, e continuar a desenvolver plataformas de cooperação"[318].

No que respeita à cooperação internacional, o "Centro Nacional de Cibersegurança[319] consolidou a sua ação enquanto CSIRT nacional e ponto focal com os CSIRT de outros Estados, colaborando ativamente com a ENISA, de entre outras organizações e concluiu a sua filiação no *Forum of Incident Response and Security Teams* (FIRST)"[320].

Já ao nível dos utilizadores da internet na UE, os mesmos continuam particularmente preocupados "com a cibercriminalidade: 85 % concorda que o risco de ser vítima da cibercriminalidade está a aumentar"[321].

Considerando a cibersegurança como a primeira linha de defesa contra a cibercriminalidade, em 2013, a UE definiu a sua estratégia para a cibersegurança concentrada na "identificação de áreas de risco elevado, na colaboração com o setor privado para colmatar

---

[315]"A Estratégia da UE para a Cibersegurança define a abordagem estratégica da UE na prevenção e resposta a ataques e perturbações que afetem os sistemas de telecomunicações da Europa", bem como "comunicar a ocorrência de ciberincidentes significativos. A lista destas entidades inclui os motores de pesquisa, os serviços de computação em nuvem, as redes sociais, as AP's, as plataformas de pagamento em linha, como o *PayPal*, e os grandes sítios *Web* de comércio eletrónico, como a Amazon". LOPES – ***Op cit.*** p. 42.

[316] CONSELHO DA UNIÃO EUROPEIA. **Cibersegurança na Europa: regras mais rigorosas e uma melhor proteção.** [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL:http://www.consilium.europa.eu/pt/policies/cyber-security/.

[317] MASSENO, Manuel – **Segurança e Liberdade na Sociedade Global em Rede.** [s.d.]. Slide 13.

[318] A "UE apoiará a cibercooperação política, operacional e técnica entre EM, designadamente no domínio da análise e gestão das consequências, e promoverá avaliações partilhadas entre estruturas da UE e instituições competentes dos EM", ao mesmo tempo que terá de reforçar "a cooperação em matéria de cibersegurança com parceiros essenciais como os EUA e a OTAN". UNIÃO EUROPEIA – ***Op cit.*** 2016. p. 17.

[319] O CNCS funciona no âmbito das "atribuições do Gabinete Nacional de Segurança, com a missão de contribuir para que Portugal use o ciberespaço no respeito pelos princípios e objetivos da Estratégia Nacional de Segurança do Ciberespaço, exercendo poderes de autoridade nacional em matéria de cibersegurança". SISTEMA DE SEGURANÇA INTERNA – **Relatório Anual de Segurança Interna de 2018.** Lisboa: Ministério da Administração Interna, 2019. p. 135.

[320] SISTEMA DE SEGURANÇA INTERNA – ***Op cit.*** 2018. p. 130.

[321] Inquérito Eurobarómetro sobre a cibersegurança, publicado em fevereiro de 2015.UNIÃO EUROPEIA – **Agenda Europeia para a Segurança.** COM(2015) 185. Estrasburgo, 2015. p. 14.

lacunas e na introdução de formação especializada"[322]. Para tal, a UE começou a trabalhar numa proposta de diretiva relativa à segurança das redes e da informação, a Diretiva NIS[323], a qual foi entretanto aprovada e que será dissecada mais à frente.

Contudo, já em 2004, a cibersegurança fazia parte da agenda da UE, tendo sido estabelecida nesse ano a *European Network and Information Security Agency*[324] (ENISA) com o "objetivo de facilitar a transição para um conhecimento partilhado e melhorar as práticas entre os EM, sendo esta questão reforçada em 2007 na agenda política da Organização, juntamente com a OTAN e outros atores do SI que se viram forçados a repensar a sua estratégia de segurança na sequência dos ataques de *DDoS* a infraestruturas públicas e privadas na Estónia"[325].

Após os ataques à Estónia, a Comissão Europeia[326] (CE) começou a abordar a questão dos ciberataques como um tema da sua própria segurança, consolidando um conjunto de diretivas e regulamentos relacionados com questões cibernéticas. Assim, em 2013, a CE publicou a *Cybersecurity Strategy*[327], a par com a "Diretiva NIS", que tenta abordar alguns dos problemas centrais da política de cibersegurança[328].

---

[322] UNIÃO EUROPEIA – ***Op cit.*** 2015. p. 21.

[323] A aplicação desta diretiva possibilitou não só a promoção de uma melhor cooperação entre as autoridades policiais e as autoridades responsáveis pela cibersegurança, como reforçou também as capacidades em matéria de cibersegurança das autoridades competentes dos EM e aumentou a notificação transnacional de incidentes.

[324] "A agência europeia para a segurança das redes e da informação (ENISA) também colabora na resposta da UE às questões de cibersegurança, trabalhando no sentido de um elevado nível de segurança das redes e da informação." UNIÃO EUROPEIA – ***Op cit.*** 2015. p. 21.

[325] CHRISTOU, G. – **The EU's Approach to Cyber Security.** Colchester: University of Essex, 2017. [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf.

[326] "A CE ajuda a moldar a estratégia geral da UE, propõe novas leis e políticas da UE, monitoriza a sua implementação e faz a gestão do orçamento da UE." A CE desenvolve e implementa políticas da UE através de: propor leis ao PE e ao Conselho da UE; ajudar os países da UE a implementar a legislação da UE; gerir o orçamento da UE e alocar financiamento; garantir, em conjunto com o Tribunal de Justiça, o cumprimento da legislação da UE; representar a UE fora da Europa, juntamente com o serviço diplomático da UE, o Serviço Europeu para a Ação Externa. Tradução livre do autor. DEFENCE – ***Op cit.*** p. 74.

[327] Refira-se que a *Cybersecurity Strategy* (Estratégia de Cibersegurança da UE) possuía três motivações: (1) em primeiro lugar, o facto de a prosperidade económica da UE estar cada vez mais dependente dos seus sistemas de informação e comunicação, implica a necessidade de um ciberespaço aberto, seguro e protegido; (2) a segunda motivação diz respeito aos objetivos políticos da União, isto é, torna-se essencial conceber e adotar um modelo de governação *multi-stakeholder*, tendo este modelo como objetivo colmatar a lacuna de capacidades europeias em matéria de cibersegurança; (3) por último, a defesa da democracia, do Estado de Direito e dos direitos fundamentais, deve ser também aplicado no ciberespaço. MEULEN, N.; JO, E.; SOESANTO, S. – **Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.** Justice, Freedom and Security, 2015. [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://dx.doi.org/10.7249/RR1354.p. 1-152. e ALMEIDA – ***Op cit.*** [s.d.]. p. 283.

[328] CAVELTY, M. – **A Resilient Europe for an Open, Safe and Secure Cyberspace.**UI Ocasional Papers 23, 2013. [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/a-resilient-europe-for-an-open-safe-and-secure-cyberspace-ilovepdf-compressed.pdf. p. 3-13.

Deste modo, a Estratégia de Cibersegurança da UE "articula a visão da UE de cibersegurança em torno de cinco prioridades: (i) alcançar a resiliência cibernética; (ii) reduzir drasticamente o cibercrime; (iii) desenvolver políticas e capacidades de ciberdefesa relacionadas com a PCSD; (iv) desenvolver os recursos tecnológicos e industriais para a cibersegurança; e finalmente (v) estabelecer uma política internacional coerente do ciberespaço da UE e promover os valores da União"[329].

Tal como já referimos, a gestão da cibersegurança através da supervisão centralizada a nível europeu não é viável[330], pelo que os governos nacionais são "os principais responsáveis pela manutenção de um bom nível de segurança e devem cooperar a nível da UE em caso de riscos e violações de segurança que ultrapassam as fronteiras nacionais"[331].

Neste sentido, ao nível da Estratégia da UE para a Cibersegurança, as estruturas envolvidas na manutenção da segurança cibernética estão organizadas em três áreas fundamentais: segurança de redes e informações (NIS), aplicação da lei e defesa[332].

Para tal, a CE procura que os seus EM adquiram capacidades cibernéticas, nas quais se incluem a "criação de um enquadramento político-jurídico no âmbito da segurança dos sistemas de informação e de comunicação dos Estados, o desenvolvimento de operações de simulação de ciberataques em grande escala e o estabelecimento de linhas diretas de denúncia de conteúdos *online* ofensivos ou prejudiciais"[333].

Nesta perspetiva, e considerando-se a Estratégia de Cibersegurança uma prioridade da política europeia atual, importa de seguida referir as entidades europeias responsáveis por tal desiderato. Assim, ao nível Europeu existem "várias agências e organizações que visam a proteção e garantia da segurança do ciberespaço, bem como dos seus utilizado-

---

[329] BARBOSA – ***Op cit.*** p. 15.

[330] A manutenção de um bom nível de cibersegurança no contexto da UE envolve setores díspares com jurisdições e responsabilidades diferentes, tanto a nível nacional quanto da UE.

[331] Tradução livre do autor. BALDONI, Roberto – Critical Infrastructure: Definitions and Concepts. In **Protecting National Critical Infrastructures from Cyber Threats.** Rome: TENACE Project, 2014. [Consult. 15 Mar. 2018]. Disponível em WWW:<URL: http://www.dis.uniroma1.it/~tenace/. p. 8.

[332] "A estratégia europeia convida os EM à partilha de informações entre as estruturas nacionais envolvidas na segurança cibernética e o setor privado, para que possam ter uma visão abrangente dos riscos e ameaças à segurança e uma melhor compreensão das técnicas de crimes cibernéticos, a fim de responder mais rapidamente e efetivamente." *Ibidem*.

[333] Para além destas estratégias, a CE "almeja também a criação por parte dos EM de plataformas nacionais de alerta, da condução de ações de formação em segurança das redes e da informação nas escolas e o desenvolvimento das capacidades nacionais para a sensibilização e formação. Incentiva ainda a criação de Equipas de Resposta a Emergências Informáticas (CERTs) e o estabelecimento de redes nacionais de CERTs, assim como a instituição de centros de excelência em matéria de cibersegurança a nível nacional ou com outros EM. Pretende ainda a criação, juntamente com a ENISA, de planos de contingência e de cooperação, nacionais e europeus, em matéria de resposta a incidentes e recuperação em caso de catástrofes; a definição de estratégias nacionais de cibersegurança; e a criação de autoridades nacionais competentes nessa matéria." BARBOSA – ***Op cit.*** p. 14.

res"[334], das quais destacaremos as seguintes: a ENISA, a Agência Europeia de Defesa (EDA) e o Centro Europeu de Cibercrime (EC3).

Começando pela ENISA, tal como já referimos, foi em 2004 que a UE criou a mesma, fruto da necessidade de proteção e defesa do ciberespaço.

A ENISA assume-se como um "centro especializado que promove a cibersegurança na Europa, ajudando a UE e os seus EM a equiparem-se melhor e a estarem preparados para prevenir, detetar e responder a problemas de segurança da informação"[335].

Esta agência europeia é especializada em cibersegurança e tem como "missão contribuir para segurança cibernética na Europa aumentando a consciência da segurança das redes e da informação e para desenvolver e promover uma cultura, das redes e da informação na sociedade em benefício dos cidadãos, consumidores, empresas e organizações do sector público em toda a União[336]"[337].

De igual modo, a ENISA é responsável pela "elaboração de relatórios que permitam visualizar as diferentes situações que ocorrem no ciberespaço, nomeadamente, no que concerne aos sistemas críticos de cada EM e do sector privado trabalhando em estreita colaboração com os mesmos para fornecer conselhos e soluções para os problemas que possam surgir"[338], bem como trabalha no "desenvolvimento e implementação da política e da legislação da UE sobre questões relativas à cibersegurança"[339].

Assim, a ENISA tem igualmente como função "desenvolver equipas de resposta a incidentes nacionais e apoiar a realização de exercícios entre os diferentes organismos e organizações da União, bem como entre estes e terceiros"[340], com o intuito de "proteger as infraestruturas críticas da UE, propondo soluções e dando conselhos práticos a entidades dos setores público e privado dos países e instituições da União"[341].

---

[334] BARBOSA – ***Op cit.*** p. 15.
[335] Neste sentido e para "combater as ameaças no ciberespaço, até os EUA e a Rússia entraram em colaboração para concretizar, em 2013, um esforço conjunto para a criação um grupo de trabalho bilateral com o objetivo de diminuir a insegurança internacional no campo das tecnologias de informação e comunicação." PEREIRA, Joana – O Ciberespaço e a Mutação da Realidade: o caso dos EUA. In **IDN Brief**. Lisboa: Instituto da Defesa Nacional, IDN Publicações, 2013. ISSN 2182-5327. p. 8. e BARBOSA – ***Op cit.*** p. 15.
[336] Art.º 1º (1) do Regulamento ENISA (UE) Nº 526/2013.
[337] LEITE – ***Op cit.*** p. 10.
[338] Isto inclui, os exercícios europeus de cibersegurança, o desenvolvimento de estratégias nacionais de segurança cibernética, estudos sobre a adoção da nuvem segura, abordando questões de proteção de dados, tecnologias e privacidade reforço da privacidade das novas tecnologias, entre outros. *Ibidem*.
[339] *Ibidem*.
[340] *Ibidem*.
[341] "Desde a organização de exercícios de crise de cibersegurança internacionais, passando pelo desenvolvimento de estratégias nacionais de cibersegurança, até à promoção da cooperação entre equipas de resposta a incidentes no domínio da segurança informática e da criação de capacidades de resposta, a ENISA também publica relatórios e estudos sobre questões de cibersegurança." BARBOSA – ***Op cit.*** p. 16.

Deste modo, em 2016, a ENISA definiu os seguintes objetivos estratégicos de ação delineados para os anos de 2016-2018: "(i) desenvolver e manter um elevado nível de conhecimentos dos intervenientes da UE, tendo em conta a evolução da segurança das redes e da informação; (ii) auxiliar os EM e as instituições e corporações da União no reforço das capacidades de toda a UE; (iii) auxiliar os EM e as instituições e corporações da União no desenvolvimento e implementação das políticas e regulamentos necessários à segurança das redes e da informação; e finalmente (iv) reforçar a cooperação quer entre os EM e a União, assim como com as comunidades relacionadas com a segurança das redes e da informação"[342].

Analisando agora a Agência Europeia de Defesa (EDA), a mesma foi criada em 2004, como uma agência do Conselho da UE, apesar de apenas ter surgido em pleno após a entrada em vigor do Tratado de Lisboa e consequentemente da PCSD, que desde 2010 tem vindo a "contribuir para a defesa do ciberespaço da comunidade europeia, através do seu esforço para o desenvolvimento de capacidades neste domínio"[343].

Como tal, esta agência tem desenvolvido "capacidades humanas e tecnologias, focando-se tanto no treino de competências como nos exercícios de ciberdefesa"[344].

Deste modo, a EDA tornou-se no "centro da cooperação europeia em defesa com conhecimentos em redes, permitindo cobrir todo o espectro: desde a harmonização de requisitos até ao fornecimento de capacidades operacionais; da pesquisa e inovação ao desenvolvimento de demonstradores de tecnologia; de treino e exercícios à manutenção e suporte às operações da PCSD. Também trabalha para fortalecer a indústria de defesa europeia e atua como facilitador e interface entre as partes interessadas militares dos EM e as políticas da UE em geral, com impacto na defesa"[345].

Por último, iremos abordar o Centro Europeu de Ciberterrorismo[346] (EC3). Este Centro surgiu da constatação do aumento das ameaças no ciberespaço, devido aos avanços tecnológicos, e do inerente "sentimento de insegurança face à informação partilhada e armazenada no ciberespaço"[347].

---

[342] *Ibidem*.
[343] *Ibidem*.
[344] Considerando que este tipo de ameaças é multifacetado, esta agência "procura ainda uma coordenação entre os esforços militares e civis para o combate às ciberameaças." BARBOSA – ***Op cit.*** p. 17.
[345] Tradução livre do autor. DOMECQ, Jorge – Agência Europeia de Defesa: desenvolvimento da capacidade de defesa cibernética. In DEFENCE – ***Op cit.*** p. 92.
[346] *European Cybercrime Centre*.
[347] O Centro Europeu para o Cibercrime iniciou as suas atividades em janeiro de 2013, devido à consciência da UE como potencial alvo para ciberataques devido à quantidade de infraestruturas em rede e do comércio e pagamentos serem essencialmente digital. BARBOSA – ***Op cit.*** p. 17.

Organicamente, o EC3 está "sob a alçada da Europol[348], surgindo a sua relação com a ENISA da capacidade que o EC3 dispõe de regular as medidas protocolarmente definidas por esta entidade"[349]. Assim, o EC3 tem como finalidades "o fortalecimento da resposta da aplicação da lei da criminalidade informática na UE e ajudar a proteger os cidadãos europeus, empresas e governos e tem como principais campos de ação o auxílio aos EM para que estes consigam extinguir redes de cibercrime relacionadas com o abuso sexual de crianças, fraude informática, intrusões e *botnets*"[350].

Nesta perspetiva, o EC3 tem-se focalizado em três áreas essenciais: "(a) cibercrimes praticados por grupos organizados, particularmente aqueles que geram avultados lucros, como a fraude *online*; (b) cibercrime que causam sérios danos às vítimas, como a exploração sexual de menores *online*; (c) cibercrimes (incluindo ciberataques) que afetem infraestruturas críticas e os sistemas de informação da UE"[351].

A Estratégia de Cibersegurança da UE pretende reduzir drasticamente a cibercriminalidade, devido ao facto desta ser "uma das formas de criminalidade que mais têm aumentado, fazendo mais de um milhão de vítimas por dia em todo o mundo"[352]. Tal, acontece devido ao facto de os cibercriminosos e as redes de cibercriminalidade se estarem a tornar cada vez mais sofisticados, motivo pelo qual se afigura como necessário dispor das ferramentas operacionais corretas e de capacidades para os combater.

A potenciar o exposto, surge o facto de os cibercrimes serem altamente lucrativos e de baixo risco e, muitas vezes, os criminosos explorarem o anonimato dos domínios dos sítios *Web*. De igual modo, a cibercriminalidade não conhece fronteiras, o que reforça a

---

[348] Este Centro foi criado nos termos da estratégia de segurança interna da UE, estando o mesmo incluído na "agência europeia Europol, não só pelas qualificações atribuídas a esta agência enquanto garante da aplicação da lei e de combate ao crime, como pela cooperação entre Estados como pressuposto de uma estratégia eficaz". BARBOSA – ***Op cit.*** p. 17.

[349] "A ENISA apoia o trabalho desenvolvido pelo EC3, tendo um papel de mediador e auxiliando na articulação e aplicação da lei entre os EM, respeitante à prevenção e combate ao cibercrime. Desta forma, o EC3 entrega relatórios à ENISA que indicam as últimas metodologias de ciberataques, e que definam estratégias e medidas de combate a alvos de investigação por cibercrime." LEITE – ***Op cit.*** p. 10.

[350] *Ibidem*.

[351] "Para além destas áreas, o EC3 serve ainda como o centro da informação criminal e *intelligence*; apoia as operações e investigações dos EM, auxiliando através de meios de investigação, coordenação e análise; fornece uma variedade de produtos de análise estratégica, permitindo a tomada de decisão informada a nível tático e estratégico, sobre o combate e a prevenção de crimes cibernéticos; estabelece uma relação de cooperação entre as forças de combate ao cibercrime, com as academias e universidades, bem como com outros atores não judiciais ou académicos; apoia a formação e aquisição de competências, em especial das autoridades competentes dos EM; fornece recursos altamente especializados de apoio forense digital e técnicas de investigações e operações; e garante a aplicação da lei comunitária." BARBOSA – ***Op cit.*** p. 18.

[352] COMISSÃO EUROPEIA – **Estratégia da UE para a cibersegurança: Um ciberespaço aberto, seguro e protegido.** Bruxelas: JOIN, 2013. p. 9-10.

necessidade de as autoridades policiais adotarem uma abordagem transfronteiriça coordenada e de colaboração para responder a esta ameaça crescente.[353]

Em complemento, não esqueçamos que a cibercriminalidade é "uma realidade incontornável, em permanente mutação e num processo evolutivo constante que [pode ser classificado] como «todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo desse ato ou em que o computador é o objeto do crime»"[354],,[355].

Em relação à criminalidade grave e organizada constatamos tratar-se de "um fenómeno cada vez mais dinâmico e complexo que requer uma resposta robusta e orientada pelas informações por parte da UE, tendo por isso sido considerada pela Europol, no relatório denominado *Serious Organised Crime Threat Assessment* (SOCTA)"[356].

Este relatório tem como objetivo dar a conhecer a evolução da criminalidade grave e organizada e as ameaças que ela representa para a UE, bem como definir a cibercriminalidade como uma das áreas de criminalidade de primeira prioridade, juntamente com a droga, a falsificação, o tráfico de seres humanos, os crimes contra a propriedade, os crimes económicos, os crimes ambientais e o tráfico de armas.[357]

Este tipo de criminalidade é potenciada pela sociedade da informação, assente sobre o uso ótimo das novas TIC, em respeito pelos princípios democráticos, da igualdade e da solidariedade, a qual visa "o reforço da economia e da prestação de serviços públicos e, a final, a melhoria de qualidade de vida de todos os cidadãos"[358]. Contudo, a globalização,

---

[353] *Ibidem*.
[354] Cfr. Parecer n.º 11/2011 da Procuradoria-Geral da República. **Diário da República II Série.** N.º 109 (05-06-2012). p. 20509-20519.
[355] TEIXEIRA – ***Op cit.*** p. 10.
[356] COPETO, Rogério – **Cibercriminalidade.** [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://www.lidadornoticias.pt/opiniao-rogerio-copeto-oficial-da-gnr-cibercriminalidade/.
[357] Para a maioria da população a "cibercriminalidade está associada a crimes financeiros, onde o objetivo do cibercriminoso é a apropriação de códigos bancários, mas nenhum dado está a salvo dos cibercriminosos, verificando-se que o número e a frequência de violações de dados pessoais estão a aumentar, o que, por sua vez, está a conduzir a mais casos de fraude e extorsão, existindo uma enorme gama de oportunidades que os cibercriminosos têm procurado explorar, com recurso a diversos dispositivos: *botnets* (redes de dispositivos infetados com *malware* sem o conhecimento de seus utilizadores, com o objetivo de transmitir um vírus, com a capacidade de controlar remotamente equipamentos informáticos para furto de senhas, desativando qualquer proteção antivírus); *backdoors* (permite o acesso remoto aos dispositivos para criar *botnets* em equipamentos comprometidos, permitindo o furto de qualquer tipo de dados); fóruns *online* (permitem a troca de conhecimentos/informação entre *hackers*); *bulletproof* (serviços contra-anti-vírus); transformação de moeda corrente em virtuais; fraude *online*; (…) realização *online* de operações de venda de armas, de passaportes falsos, cartões de crédito falsificados e/ou clonados, drogas, serviços de *hackers*", entre outros. *Ibidem*.
[358] COSTA, João – **A responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na Internet – Em especial da responsabilidade pelos conteúdos gerados por utilizadores.** Porto: Faculdade de Direito da Universidade de Direito, 2011. Dissertação de Mestrado. p. 28-29.

ainda que de forma disfarçada, veio potenciar a violação da "privacidade do indivíduo nas suas mais diversas vertentes e expô-lo cada vez mais perante a sua comunidade"[359].

Outro problema a ter em consideração diz respeito ao facto da cibercriminalidade não conhecer fronteiras, bem como ser flexível e inovadora por natureza.

Com efeito, as "forças e os serviços policiais têm de ser capazes de acompanhar e antecipar a engenhosidade dos criminosos em matéria de prevenção, deteção e ação penal, [pelo que] a cibercriminalidade exige que as autoridades judiciárias competentes revejam a forma como cooperam, no âmbito das suas competências e da legislação aplicável, para assegurarem um acesso transnacional mais rápido a elementos de prova e a informações, tendo em conta atuais e futuros desenvolvimentos tecnológicos, como a computação em nuvem e a internet das coisas"[360].

A UE tem procurado legalmente controlar estes fenómenos, pelo que tem criminalizado os ataques a Redes e Sistemas Informáticos, destacando-se o seguinte:

- A Convenção do Conselho da Europa sobre o Cibercrime, adotada em Budapeste, a 23 de novembro de 2001, nomeadamente com a previsão dos tipos correspondentes aos seguintes atos: o acesso ilícito (art.º 2º); a interceção ilícita (art.º 3º); o dano provocado nos dados (art. 4º); a sabotagem informática (art.º 5º); e ainda a utilização indevida de dispositivos (art. 6º).[361] Esta Convenção "admite tanto a recolha em tempo real de dados relativos ao tráfego (art.º 20.º) quanto a interceção de dados relativos ao conteúdo (art.º 21.º), mas com as salvaguardas resultantes dos instrumentos internacionais de proteção dos Direitos Humanos, em especial da Convenção Europeia dos Direitos Humanos, e um pleno respeito pelo Princípio da Proporcionalidade (art.º 15.º)"[362].

- A Diretiva 2013/40/UE do PE e do Conselho, de 12 de agosto de 2013, relativa aos ataques contra os sistemas de informação, e que revoga a Decisão-Quadro 2005/222/JAI: o acesso ilegal a sistemas de informação (art.º 3.º); a interferência ilegal no sistema (art.º 4.º); a interferência ilegal nos dados (art.º 5.º); a interceção ilegal (art.º 6.º); e

---

[359] TEIXEIRA, Paulo – **O fenómeno do *Phishing*. Enquadramento jurídico-penal**. Lisboa: Universidade Autónoma de Lisboa, 2013. Dissertação de Mestrado. p. 1.

[360] "A recolha de provas eletrónicas em tempo real por outras jurisdições sobre questões como os proprietários de endereços IP ou outras provas eletrónicas, bem como assegurar a sua admissibilidade em tribunal, são questões essenciais, [o que] exige agentes policiais altamente qualificados para poderem acompanhar o aumento considerável do âmbito, da sofisticação e dos tipos de cibercriminalidade." UNIÃO EUROPEIA – ***Op cit.*** 2015. p. 22.

[361] MASSENO, Manuel **– Segurança e Liberdade na Sociedade Global em Rede.** Slide 28-29.

[362] MASSENO, Manuel – Garantir a Cibersegurança e a Ciberdefesa à custa dos Cidadãos? In **IX Simpósio sobre Segurança Informática e Cibercrime.** SimSIC: Beja, 2018. Slide 4.

a produção, venda, aquisição para utilização, importação, distribuição ou outra forma de disponibiliza os dispositivos/instrumentos utilizados para cometer as infrações (art. 7º).[363]

Uma tipologia criminal ligada ao ciberespaço é o crime de falsidade informática, o qual tem como *modus operandi* a captura por grupos criminosos de elementos bancários dos utilizadores dos serviços de *homebanking*, através da "criação de páginas da *Web* ou domínios (*sites*) em tudo idênticos a determinadas instituições de crédito, de forma a induzirem o comum utilizador/cliente de um banco específico a aceder a essa página, crendo este que passa assim a estar a aceder ao *site* institucional do seu banco"[364].

Este crime de falsidade informática é um crime de natureza pública, pelo que não se exige a apresentação da respetiva queixa-crime para que o procedimento criminal seja iniciado, bastando a mera comunicação dos factos. Nesta tipologia criminal, o bem jurídico que se pretende proteger é a segurança nas relações jurídicas[365].

A segurança das redes e dos sistemas de informação é outro tema de particular importância para a UE.

Desta feita, em 2016, a CE propôs o primeiro quadro[366] regulamentar da UE de segurança cibernética, no que se refere à segurança das redes e dos sistemas de informação, a qual foi adotada pelo PE em julho de 2016 e fornece medidas legais para melhorar e reforçar o nível geral de cibersegurança em toda a UE.[367]

Assim, em 17 de maio de 2016, o Conselho implementou novas regras para aumentar a segurança das redes e dos sistemas de informação, através da criação da diretiva sobre a segurança das redes e da informação (SRI), a qual veio reforçar a cooperação entre os EM no âmbito da cibersegurança[368].

A Diretiva NIS visa alcançar um alto padrão de segurança de redes e sistemas de informação em toda a UE, pelo que se concentra principalmente na regulamentação de operadores de serviços essenciais (em setores críticos como a energia, os transportes, a

---

[363] *Ibidem*.
[364] TEIXEIRA – ***Op cit.*** p. 19.
[365] Sempre que o documento falsificado é colocado no tráfico jurídico, estamos perante um caso de falsidade informática. MONIZ, Helena – **O Crime de Falsificação de documentos. Da falsificação intelectual e da falsificação em documento.** Coimbra: Coimbra Editora, 2004. p. 269. e TEIXEIRA – ***Op cit.*** p. 19.
[366] Este quadro "foi desenvolvido para aumentar a resiliência, melhorando as capacidades nacionais de cibersegurança; promover uma melhor cooperação entre os EM; e exigindo que empresas de setores económicos importantes adotem uma mitigação eficaz de riscos e relatem incidentes graves às autoridades nacionais".
[367] Tradução livre do autor. DEFENCE – ***Op cit.*** p. 56.
[368] CONSELHO DA UNIÃO EUROPEIA – **Conselho aprova regras em matéria de cibersegurança a nível da UE.** [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL:http://www.consilium.europa.eu/pt/press/pressreleases/2016/05/17widecybersecurityruleadopted/.

saúde, as finanças e a assistência médica) e de provedores de serviços digitais (serviços de computação em nuvem, mercados *online* e mecanismos de busca). Para estas organizações, a Diretiva NIS destaca duas obrigações principais para garantir a continuidade dos serviços essenciais e evitar apagões em larga escala: 1. adotar medidas técnicas e organizacionais apropriadas para gerir ameaças a redes e sistemas de informação; 2. notificar as autoridades 'sem demora injustificada' de qualquer incidente de segurança significativo.[369]

Esta Diretiva preconiza que todos os EM estabeleçam uma equipa nacional / governamental de resposta a incidentes, a qual é designada como Equipa de Resposta a Emergências por Computador (CERT). As CERTs têm por missão ajudar os governos a proteger a infraestrutura de informações críticas e desempenhar um papel fundamental na coordenação da gestão de incidentes com as partes interessadas relevantes em nível nacional[370].

Assim, a criação destas Equipas teve como objetivo permitir uma reação rápida a ciberameaças e ciberincidentes e estabelecer igualmente "um Grupo de Cooperação entre os EM, com vista a apoiar e facilitar a cooperação estratégica e o intercâmbio de informações, bem como o desenvolvimento de um clima de confiança".[371]

Em 2017 verificou-se a atualização da Estratégia de Cibersegurança da UE, devido à evolução do ambiente global de ameaças cibernéticas, entre as quais destacamos: "operações cibernéticas disruptivas contra infraestruturas críticas, instituições democráticas e a 'Internet das Coisas' (*IoT*), e ataques massivos de redes de *bots* e casos globais de *ransomware*, como *WannaCry* e *NotPetya"*[372]. As referidas ameaças aumentaram a consciencialização sobre os riscos cibernéticos, o que levou à necessidade da UE se adaptar à nova realidade e adotar uma abordagem mais proativa em relação às ameaças cibernéticas.

Em 17 de maio de 2019, o Conselho da UE adotou a Decisão (PESC) 2019/797 e o Regulamento (UE) 2019/796 do Conselho que impõem medidas restritivas contra ciberataques que ameacem a União ou os seus EM. A nova legislação evoluiu das conclusões de um quadro para uma resposta diplomática conjunta a atividades cibernéticas maliciosas (a *Cyber Diplomacy Toolbox*), adotada pelo Conselho em 19 de junho de 2017, e estabeleceu

---

[369] Deseja-se que a implementação da Diretiva NIS leve a um aumento geral da segurança cibernética nos setores considerados vitais para a economia e o Estado. Tradução livre do autor. DEFENCE – ***Op cit.*** p. 57.
[370] Assim, esta "Diretiva define a responsabilidade dos EM não apenas de trocar informações sobre incidentes cibernéticos a nível da UE, mas também de desenvolver e implementar estratégias e estruturas nacionais apropriadas de cibersegurança para a segurança de redes e sistemas de informação." Tradução livre do autor. DEFENCE – ***Op cit.*** p. 58.
[371] A Comissão assinou um acordo em 2016 em Bruxelas com a indústria sobre cibersegurança e intensificou os esforços para combater as ciberameaças. [Consult. 15 Mar. 2018]. Disponível em WWW:<URL: http://europa.eu/rapid/pressrelease_IP162321_pt.htm.
[372] Tradução livre do autor. DEFENCE – **Op cit.** p. 24.

um quadro de medidas contra possíveis agressores. Com base na caixa de ferramentas e nos seus princípios, a decisão e o regulamento do Conselho de maio de 2019 constituem um importante passo em frente para enfrentar as ameaças emergentes à segurança no ciberespaço a nível da UE.[373]

No sentido de impor sanções, a UE veio assim definir diversas ações que significam a ocorrência de um ataque cibernético, nas quais se incluem: "(a) acesso a sistemas de informação; (b) interferência no sistema de informação; (c) interferência de dados; ou (d) interceptação de dados. As sanções podem ser impostas para responder não apenas às ações concluídas, mas também às ações tentadas. Para estar sujeito a sanções, um ataque cibernético deve atender a dois critérios: (a) o ataque tem um efeito significativo; e (b) o ataque constituir uma ameaça externa para a União ou seus EM"[374].

Em complemento, já para se considerar que um ataque cibernético tem um efeito significativo, uma série de indicadores deve ser considerada: "(a) o escopo, a escala, o impacto ou a gravidade da interrupção causada; b) o número de pessoas singulares ou coletivas, entidades ou organismos afetados; c) o número de EM em causa; (d) a quantia de perda económica causada; (e) o benefício económico obtido pelo autor, para si ou para terceiros; (f) a quantidade ou natureza dos dados roubados ou a escala das violações de dados; e (g) a natureza dos dados comercialmente sensíveis acedidos"[375].

Por outro lado, a "segunda condição de constituir uma ameaça externa é cumprida quando um ataque (a) tem origem ou é realizado de fora da União; (b) utilize infraestruturas fora da União; c) é realizada por qualquer pessoa singular ou coletiva, entidade ou organismo estabelecido ou que opera fora da União; ou d) for realizado com o apoio, sob a direção ou sob o controlo de qualquer pessoa singular ou coletiva, entidade ou organismo que opere fora da União"[376]. Porém, "outras pessoas, entidades e organismos – originários e que operam na UE – permanecem sujeitos à jurisdição nacional. Esta é uma diferença

---

[373] A legislação foi promovida especialmente pelo Reino Unido e pela Holanda, que sofreram grandes ataques cibernéticos nos meses anteriores à adoção da decisão. No caso do Reino Unido, os serviços de inteligência do Reino Unido reuniram e apresentaram evidências de uma campanha coordenada de *hackers* conduzida pelo grupo estatal chinês *Advanced Persistent Threat* 10 (APT 10). Embora os EM tenham considerado uma resposta diplomática conjunta contra o grupo *hacker*, eles só conseguiram adotar uma declaração do Conselho em que o APT 10 não foi mencionado diretamente. No entanto, apenas um mês depois, o Conselho adotou uma legislação que permitia à UE impor medidas restritivas (expressão que a UE usa para se referir às suas sanções) contra agressores no ciberespaço. BOTEK, Adam – **Regime Sancionatório da UE para ataques cibernéticos.** Agência Nacional de Segurança da Informação e Cibernética da República Checa. CCD-COE – INCYDER. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/.

[374] *Ibidem*.

[375] *Ibidem*.

[376] *Ibidem*.

importante do regime das sanções antiterroristas da UE, que também pode ser imposto a cidadãos ou entidades da UE como a ETA, o IRA e os seus membros"[377].

De igual modo, as sanções podem ser aplicadas não apenas contra indivíduos diretamente responsáveis por ataques cibernéticos, mas contra todos os indivíduos que fornecem suporte financeiro, técnico ou material ou que estejam envolvidos num ataque cibernético e todos os assuntos associados aos envolvidos[378].

As diversas sanções que a UE pode impor são duplas. A primeira é a prevenção da entrada dos territórios sancionados ou de trânsito nos territórios dos EM da UE. A segunda é o congelamento de fundos e recursos económicos: nenhum fundo ou recurso económico deve ser disponibilizado direta ou indiretamente para o benefício dos visados[379].

Após esta análise ao panorama da UE, iremos ver de seguida o panorama nacional.

Assim, refira-se que, desde logo, Portugal foi um dos pioneiros no combate à criminalidade informática, sendo que já em 1991 aprovou a Lei n.º 109/91, de 17 de agosto, denominada de Lei da Criminalidade Informática[380].

No que respeita às tendências da cibercriminalidade em Portugal em 2013, uma das realidades criminais mais denunciadas era a da criação de falsos perfis em redes sociais, com o nome de outra pessoa, a fim de posteriormente injuriá-la, difamá-la ou relatar factos da sua vida privada ou denegridores da sua imagem. Por regra, "tais situações têm sido enquadradas como injúrias/difamações ou como devassa da vida privada (art.º 193º do CP) ou, ainda como divulgação de fotografias (art.º 199º, nº 2, alínea b) do CP)"[381].

---

[377] *Ibidem*.

[378] Os ataques cibernéticos podem ser dirigidos à UE (suas instituições, órgãos ou escritórios, suas delegações em países terceiros ou organizações internacionais, suas operações e missões comuns de política de segurança e defesa ou seus representantes especiais) ou a um EM (sua organização, infraestruturas críticas, serviços necessários para a manutenção de atividades sociais e / ou económicas essenciais, funções críticas do Estado, armazenamento ou processamento de informações classificadas e equipas governamentais de resposta a emergências). Nos casos em que é necessário alcançar um objetivo da política comum de segurança e defesa da UE, também podem ser impostas sanções como resposta a ataques cibernéticos com efeito significativo contra Estados terceiros ou organizações internacionais. *Ibidem*.

[379] As sanções podem ser dirigidas apenas contra pessoas físicas ou jurídicas, outras entidades ou órgãos diferentes de um Estado (ou seja, atores não estatais), pelo que os atores estatais permanecem fora do escopo do regime de sanções. A UE abstém-se de atribuir ataques cibernéticos a Estados terceiros, afirmando que esta será uma decisão política soberana que cada EM deve considerar caso a caso. *Ibidem*.

[380] "Esta lei visava a penalização de condutas como a falsidade informática, o dano relativo a dados ou programas informáticos, a sabotagem informática, o acesso ilegítimo, a interceção ilegítima e a reprodução ilegítima de programa protegido. Esta lei vigorou até ao ano de 2009, altura em que surge a nova Lei do Cibercrime (Lei 109/2009 de 15 de setembro), que veio substituir a anterior. Esta nova lei surge por força da Decisão-Quadro nº 2005/222/JAL do Conselho da Europa, de 24 de fevereiro relativa a ataques contra sistemas de informação, e da necessidade de adaptação da legislação nacional à Convenção sobre o Cibercrime do Conselho da Europa." BARBOSA – ***Op cit.*** p. 19.

[381] PROCURADORIA-GERAL DA REPÚBLICA – **Gabinete Cibercrime. Relatório da Actividade.** Lisboa: Procuradoria-geral da República – Gabinete Cibercrime, 2013. p. 5-6.

Nesta altura, eram igualmente apontadas como "questões referentes a dificuldades na investigação: a dificuldade na compreensão dos conceitos e das regras referentes à obtenção de prova digital, apesar de, em geral, se assumir a sua crescente relevância, num número cada vez maior de processos"[382], entre outras.

No seguimento, Portugal tem procurado a construção de um ciberespaço seguro e sustentável, "através de um esforço conjunto e de uma partilha de responsabilidades [que envolvem] o governo, a AP, as FA, as empresas e os cidadãos na promoção de medidas de proteção e segurança do ciberespaço"[383]. Deste modo, o "desenvolvimento da ENCS funcionou como um pontapé de saída para a tomada de consciência relativamente à necessidade de proteção e salvaguarda dos interesses nacionais e das IC"[384].

A problemática da Cibercriminalidade em Portugal está cada vez mais na ordem do dia, tal como concretiza a Lei que define os objetivos, prioridades e orientações de política criminal para o biénio de 2017-2019, em cumprimento da Lei n.º 17/2006, de 23 de maio, que aprova a Lei-Quadro da Política Criminal, a qual veio definir a Cibercriminalidade como um dos crimes de prevenção prioritária (art.º 2º, alínea c)) e um dos crimes de investigação prioritária (art.º 3º, alínea g)), de acordo com a Lei n.º 96/2017[385], de 23 de agosto.

Em Portugal, a matéria da criminalidade informática está regulada dispersamente por vários diplomas, nomeadamente: no Código Penal, na Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro), na Lei da Proteção de Dados Pessoais (Lei n.º 58/2009, de 08 de agosto), na Lei da Proteção Jurídica de Programas de Computador (Decreto-Lei n.º 252/94[386], de 20 de outubro), no Código de Direitos de Autor e dos Direitos Conexos (Decreto-Lei n.º 63/85[387], de 14 de março) e no Regime Geral das Infrações Tributárias (Lei n.º 15/2001[388], de 05 de junho).[389]

---

[382] "a) Nalguns casos, estas dificuldades resultam de incoerências ou inconsistências do sistema legislativo. Assim acontece, por exemplo, pela dificuldade de conciliação entre a Lei nº 32/2008, referente à retenção de dados, e a Lei do Cibercrime (Lei nº 109/2009). Ou, também por exemplo, pela dificuldade prática de, no articulado da Lei nº 32/2008, distinguir entre dados de assinante e dados de tráfego. As discussões a este propósito culminam, em regra, na conclusão da necessidade de ajustamento legislativo. b) Noutros casos, as dificuldades resultam da natureza das investigações e do ecossistema em que se desenrolam. Foi referida a impossibilidade de ter sucesso na identificação de suspeitos, se estes utilizarem servidores *proxy*, que em termos práticos tornam as suas comunicações quase anónimas. O mesmo se diga de suspeitos que utilizem pontos de acesso públicos à internet (juntas de freguesia, bibliotecas públicas ou hotéis, por exemplo)." PROCURADORIA-GERAL DA REPÚBLICA – ***Op cit.*** p. 7 e 8.

[383] ALMEIDA – ***Op cit.*** [s.d.]. p. 285.

[384] *Ibidem*.

[385] Lei N.º 96/2017. **Diário da República I Série.** N.º 162 (23-08-2017), p. 4924-4928.

[386] Retificado pela Declaração de Retificação n.º 2-A/95, e alterado pelo Decreto-Lei n.º 334/97, de 27 de novembro.

[387] Alterado, entre outras, pela Lei n.º 49/2015, de 05 de junho.

[388] Alterada, entre outras, pela Lei n.º 82-E/2014, de 31 de dezembro.

Em complemento, refira-se que Portugal "se viu obrigado a adotar uma estratégia que visasse a promoção da proteção das suas redes de comunicação e infraestruturas críticas, [uma vez que] uma boa parte da administração central do Estado encontra-se informatizada, partilhando e armazenando uma grande parte da informação no ciberespaço"[390].

Quanto à LC, registe-se que a mesma "sistematiza grande parte das normas penais e processuais relativas ao espetro do cibercrime e da recolha da prova digital, ao mesmo tempo que introduziu novas tipologias de crime informático e abarcou os três tipos de crime no ciberespaço já referidos anteriormente"[391]. Assim, esta Lei pretende "regular a utilização do ciberespaço, estabelecendo limites de atuação aos possíveis perpetradores e definindo os propósitos e a conduta da investigação criminal em matéria de cibersegurança"[392].

O surgimento da mesma teve por base as profundas mudanças tecnológicas ocorridas entre o início da década de noventa do século XX e os primeiros nove anos do novo milénio, factualidades que levaram a Lei da Criminalidade Informática de 1991 a tornar-se deficitária e, por isso, desadequada às necessidades securitárias do século XXI. Neste sentido, a "alteração do entendimento relativamente aos comportamentos no ciberespaço que deveriam ser considerados crime informático, obrigaram à criação de normas jurídicas relacionadas com tais comportamentos, relativos ao incentivo, auxílio, cumplicidade e tentativa, bem como a responsabilidade de indivíduos ou pessoas coletivas, competência territorial e ainda o intercâmbio de informação, o que viria a implicar a revogação da Lei n.º 109/91, de 17 de agosto de 1991"[393].

A ratificação do tratado da Convenção de Budapeste sobre Cibercrime (CBC) em maio de 2009 levou a que Portugal viesse a acolher as obrigações legislativas decorrentes da Convenção, o que se materializou na criação pela Assembleia da República da Lei n.º 109/2009, de 15 de setembro de 2009. Assim, a referida Lei veio a estabelecer as disposições relativas à cooperação internacional em matéria penal, relativas ao crime informático e a recolha de indícios criminais em suporte digital, bem como as disposições penais mate-

---

[389] DIAS – ***Op cit.*** p. 83.
[390] "Nos últimos anos temos vindo a assistir a uma desmaterialização dos processos e a uma passagem da AP para o espaço virtual, sendo várias as instituições públicas dependentes de plataformas *online* para trabalhar internamente e para interagir com os cidadãos e empresas. Assume-se, com esta nova informatização administrativa, uma cada vez maior e crescente necessidade de proteger e assegurar não só o bom funcionamento destas instituições, como a integridade da informação detida pelas mesmas." BARBOSA – ***Op cit.*** p. 18.
[391] BARBOSA – ***Op cit.*** p. 19.
[392] "Esta lei estabeleceu assim o regime penal para os crimes de natureza informática, porém, o combate aos ciberataques ou a promoção da segurança do ciberespaço engloba outras atitudes e políticas públicas que vão para além da criminalização dos atos, presentes em estratégias e diretivas de atuação." *Ibidem*.
[393] VERDELHO, Pedro – **A nova Lei do Cibercrime.** Scientia Juridica, 2009. 320(58). p. 717-749.

riais e processuais[394]. Neste sentido, na sequência das alterações promovidas pela referida norma legal, foram definidas as disposições materiais: falsidade informática; dano relativo a programas ou outros dados informáticos[395]; sabotagem informática[396]; acesso ilegítimo[397]; interceção ilegítima[398]; e reprodução ilegítima de programa protegido[399].[400]

De igual modo, tal como já estudamos, a RCM n.º 115/2017, de 24 de agosto, com base na RCM n.º 36/2015, de 12 de junho, veio aprovar a ENSC, com o intento de aprofundara segurança das redes e da informação e, em especial, garantir a proteção e a defesa das IC e dos serviços vitais de informação.[401] Assim, esta Resolução surgiu da necessidade "de criação de uma estratégia nacional (…) no seguimento da compreensão por parte do Estado que tanto ele como a sociedade que governa estão fortemente dependentes das TIC e que estas têm vindo a revelar-se tão promissoras quanto perigosas"[402].

Com efeito, podemos afirmar que a ENSC assenta "no compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das IC e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas"[403]. Deste modo, o seu desenvolvimento sustenta-se nos seguintes "objetivos estratégicos: (a) promover uma utilização consciente, livre, segura e eficiente do ciberespaço; (b) proteger os direitos fundamentais, a liberdade de expressão, os dados pessoais e a privacidade dos cidadãos; (c) fortalecer e garantir a segurança do ciberespaço, das infraestruturas críticas e dos serviços vitais nacionais; e (d) afirmar o ciberespaço como um domínio de desenvolvimento económico e de inovação. Por sua vez, estes objetivos estratégicos resultam em seis eixos de intervenção específicos, cujas linhas de orientação levarão a uma efe-

---

[394] Lei N.º 109/2009. **Diário da República I Série.** N.º 179 (15-09-2009). p. 6319-6325.
[395] Art.º 4.º da Lei n.º 109/2009.
[396] Art.º 5.º da Lei n.º 109/2009.
[397] Art.º 6.º da Lei n.º 109/2009.
[398] Art.º 7.º da Lei n.º 109/2009.
[399] Art.º 8.º da Lei n.º 109/2009.
[400] ALMEIDA, Cláudia – A Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço. In **III Seminário IDN Jovem.** N.º 30. Lisboa: IDN, [s.d.]. p. 278.
[401] Resolução do Conselho de Ministros n.º 115/2017. **Diário da República I Série.** N.º 163 (24-08-2017). p. 5037.
[402] Considerando a necessidade de proteger "a soberania nacional, assegurando a autonomia política e estratégica do País, bem como o crescente número de incidentes e ataques maliciosos, impõe que a segurança do ciberespaço seja considerada como uma prioridade nacional. Esta Resolução considera assim como fundamental e prioritária a efetivação de uma ENSC, estabelecendo objetivos e linhas de ação que façam uma eficaz gestão de crises e permitam a coordenação da resposta operacional a ciberataques, numa cooperação com as organizações infra e supranacionais. O texto normativo refere ainda a necessidade de reforço e aumento da resiliência das infraestruturas críticas como fundamental para uma eficaz política de combate à criminalidade no ciberespaço." BARBOSA – ***Op cit.*** p. 19-21.
[403] BARBOSA – ***Op cit.*** p. 21.

tiva segurança do ciberespaço, a reter: (i) a estrutura de segurança do ciberespaço; (ii) o combate ao cibercrime; (iii) a proteção do ciberespaço e das infraestruturas; (iv) a educação, sensibilização e prevenção; (v) a investigação e desenvolvimento; e (vi) a cooperação"[404].

Mais recentemente, foi aprovada a RCM n.º 92/2019, de 05 de junho, devido ao rápido desenvolvimento intrínseco do ciberespaço e, consequentemente, à crescente evolução das ameaças, das vulnerabilidades, dos processos e das infraestruturas, bem como dos modelos económicos, sociais e culturais que assentam na sua utilização.[405]

Na base da elaboração desta Resolução esteve igualmente a aprovação da Lei n.º 46/2018, de 13 de agosto, a qual veio estabelecer o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União. Através dessa Lei, foi instituído o Conselho Superior de Segurança do Ciberespaço, enquanto órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço.

A supracitada RCM veio assim definir a ENSC para um período de duração entre 2019 e 2023, o que permitirá tornar Portugal num país mais seguro, através da ação inovadora e resiliente que preserve os valores fundamentais do Estado de Direito e garanta o regular funcionamento das Instituições[406].

Para concluir, deixamos aqui alguns daqueles que consideramos serem os desafios de uma "visão alargada da cibersegurança, de forma a cobrir todas as dimensões de segurança que afetam o ciberespaço"[407]. Em particular:

1. Os "desafios da Diretiva NIS para o Estado, operadores privados de serviços essenciais e prestadores de serviços digitais: i) trata-se da primeira legislação da UE sobre cibersegurança, que estabelece um conjunto de medidas para prevenir incidentes cibernéticos na Europa; ii) os operadores das IC de alguns setores (serviços financeiros, transportes, energia, saúde), os facilitadores de (responsáveis pelos) serviços da sociedade da informação (tais como lojas de aplicações em linha, plataformas de comércio eletrónico, pagamentos

[404] *Ibidem*.
[405] Resolução do Conselho de Ministros n.º 92/2019. **Diário da República I Série.** N.º 108 (05-06-2019). p. 2088-2095.
[406] Comunicado do Conselho de Ministros de 23 de maio de 2019. [Consult. 06 Mar. 2020]. Disponível em WWW:<URL: https://www.portugal.gov.pt/pt/gc21/governo/comunicado-de-conselho-de-ministros?i=278.
[407] INSTITUTO DE CIÊNCIAS JURÍDICO-POLÍTICAS – **Direito da Cibersegurança e do Ciberespaço.** [Em Linha]. Lisboa: Faculdade de Direito da Universidade de Lisboa, 2018. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.icjp.pt/cursos/14278/programa?language=en.

na internet, computação em nuvem, motores de pesquisa e redes sociais) e as administrações públicas devem adotar práticas de gestão do risco e notificar os incidentes de segurança graves ocorridos nos seus serviços essenciais"[408].

2. As "dificuldades de regulação do ciberespaço: anonimato, jurisdição e extraterritorialidade, problemas agravados pela diversidade motivacional das condutas"[409].

3. O "papel das TIC na segurança do Estado e na justiça, considerando as novas metodologias de investigação, cooperação policial e formas rápidas e eficientes de obter dados: i) videovigilância, escutas, metadados, *drones,* etc; ii) as exigências de meios de investigação e probatórios decisivos mas, eventualmente colidentes, com a Constituição Penal e Processual Penal"[410].

4. O "Direito Internacional aplicável a operações em rede, procurando encontrar o posicionamento possível para os Estados no ciberespaço. As novas fronteiras geradas pelos sistemas de filtragem e encriptação, bem como a nova configuração de conceitos como soberania, ataque armado e uso da força. A alteração do equilíbrio de forças, com o surgimento de atores não estaduais a assumir atividades dos Estados"[411].

2.1.2. O Cibercrime e a sua investigação

"O anonimato perfeito torna possível o crime perfeito."

Lawrence Lessig

Atualmente, a internet desempenha um papel absolutamente fundamental em "todas as infraestruturas estratégicas e nevrálgicas do país, como governamentais, militares, de segurança, económicas, de telecomunicações, de transportes, educacionais, energéticas, de saúde e serviços de socorro e emergência"[412].

Nesta perspetiva, a internet assumiu-se como um "cibermundo sem fronteiras espaciais, territoriais, sociais, económicas, culturais, etárias, linguísticas e raciais, surgindo a chamada Sociedade da Informação"[413]. De igual modo, a internet poderá constituir-se

[408] *Ibidem*.
[409] *Ibidem*.
[410] *Ibidem*.
[411] *Ibidem*.
[412] Mas a sua importância não se fica por aqui pois estende-se a todo o tipo de relações, como as comerciais, negociais, empresariais, financeiras e económicas, e com o nascimento das redes sociais, blogues e fóruns, passou a fazer parte da vida social, pessoal e dos tempos livres dos utilizadores. DIAS, Vera – A Problemática da Investigação do Cibercrime. In **Data Venia. Revista Jurídica Digital**. N.º 1. Julho-Dezembro 2012 p. 63-88. ISSN 2182-8242. p. 64.
[413] "Para a tão falada globalização contribuíram outros fatores como as telecomunicações e as redes de transportes, mas foi com a internet que nasceu a sociedade global, caraterizada pela interligação mundial de com-

como uma fonte potencial de riscos, nos quais se incluem igualmente a segurança dos dados pessoais[414].

A importância da internet no nosso quotidiano, torna "imperiosa a necessidade de se proteger a informação para que a sua utilização abusiva não venha a servir interesses ilegítimos e atentatórios dos direitos, liberdades e garantias dos cidadãos"[415].

Não obstante vivermos "numa época dominada pelo virtual, contudo, as ameaças que esta dimensão aparentemente inócua encerra, são bem reais, [uma vez que] o ciberespaço domina a vida de milhões de indivíduos, empresas e instituições governamentais"[416].

Assim, verificamos que a internet é uma fonte de ameaças, considerando que se verificam todo o "género de práticas de índole delituosa, subversiva e beligerante, em que se enquadra desde a simples delinquência juvenil até ao hactivismo, o cibercrime, o crime organizado, a ciberpespionagem, o ciberterrorismo e a ciberguerra"[417].

Tal como já estudámos, a segurança do ciberespaço surge da necessidade de "permitir que os direitos, liberdades e garantias constitucionalizados sejam respeitados nas plataformas digitais, [pelo que] um número crescente de pessoas tem vindo a trabalhar no sentido de travar a expansão do nível de ameaças"[418].

Tal, deriva do facto de a internet ser "amplamente partilhada por empresas concorrentes, governos antagónicos e oportunistas criminosos"[419], pelo que a segurança das redes tornou-se um problema de enormes proporções.

Em complemento, diga-se que "a maioria dos problemas de segurança são intencionalmente criados por pessoas maliciosas que tentam ganhar algum benefício com isso"[420].

Neste contexto, a evolução da internet surge associada ao crescimento do cibercrime.

Historicamente, o termo cibercrime surgiu "em Lyon, na França, no final da década de 90, período em que a internet se expandia pelos países da América do Norte, num sub-

---

putadores, redes e sistemas informáticos e telemáticos. Com o aparecimento da cibernética, da digitalização e sobretudo de uma comunidade com uma cibercultura e ciberespaço próprio deu-se a evolução para a Sociedade Digital." *Ibidem*.

[414] A internet suscita certos riscos em "termos de atuações ilegais e lesivas por seu intermédio", as quais são suscetíveis de "implicar responsabilidade civil ou por violação de direitos ou por violação de normas de proteção destinadas a proteger interesses alheios (art.º 483.º do Código Civil)". LEITÃO – ***Op cit.*** p. 173-174.

[415] A UE, o Conselho da Europa, a OCDE e as NU, entre outras, "iniciaram e intensificaram o estudo e divulgação de instrumentos que consagram princípios de segurança da informação e de proteção da privacidade, tendo em vista prevenir a ilegítima utilização das tecnologias da informação". VAZ – ***Op cit.*** p. 35.

[416] RODRIGUES – ***Op cit.*** p. 3.

[417] **Portal de Cibersegurança da GNR** [Em Linha]. [Consult. 05 Out. 2019]. Disponível em WWW:<URL: http://portalciber.gnr.local/wordpress/index.php/2015/12/28/seguranca-na-internet/.

[418] TELES – ***Op cit.*** p. 14.

[419] *Ibidem*.

[420] TELES – ***Op cit.*** p. 15.

grupo das nações do G8 que analisou e discutiu os crimes promovidos via aparelhos eletrónicos ou pela disseminação de informações pela internet"[421].

O cibercrime é um processo evolutivo permanente, o qual se define como sendo "todo o ato em que o computador serve de meio para atingir um objetivo criminoso, em que o computador é o alvo desse ato ou em que o computador é o objeto do crime"[422].

De igual modo, o cibercrime poderá ser definido como "todo o ataque às TIC, às redes de comunicação e ao funcionamento das mesmas, bem como aquele que utilize estes últimos como meio para a prática de atos ilícitos"[423]. Nesta perspetiva, "consciente de que o ciberespaço poderá representar tanto o meio como o fim de um ato criminoso, a UE considera o cibercrime como todos os atos criminosos cometidos utilizando redes de comunicações eletrónicas e sistemas de informação ou contra essas redes e sistemas"[424].

O cibercrime assume-se como um "fenómeno frequente, internacional, perigoso e violador de direitos fundamentais"[425]. Para o combater é essencial "um nível de segurança, fiabilidade e eficiência no seio da internet, criando para tal uma segurança informática"[426].

Por outro lado, e de acordo com a Comunicação da Comissão ao PE, ao Conselho e ao Comité das Regiões, rumo a uma política geral de luta contra o cibercrime, esta "ameaça divide-se em três categorias de atividade criminosa diferentes, com base no tipo de atividades ilícitas que podem ser praticadas no ciberespaço"[427], a saber: "os crimes tradicionais cometidos com o auxílio do computador e redes informáticas; os crimes relacionados com o conteúdo, [designadamente,] a publicação de conteúdos ilícitos por via de meios de comunicação eletrónicos; e os crimes exclusivos das redes eletrónicas"[428].

---

[421] "O subgrupo, chamado "Grupo de Lyon", usava este termo para descrever de forma muito extensa todos os tipos de crime praticados na internet ou nas novas redes de telecomunicações que estão cada vez mais acessíveis em termos de custo." MENEZES – ***Op cit.*** p. 26.

[422] Cfr. Parecer n.º 11/2011 da Procuradoria-Geral da República. **Diário da República II Série.** N.º 109 (05-06-2012). p. 20509-20519.

[423] BARBOSA – ***Op cit.*** p. 9.

[424] *Ibidem*.

[425] A evolução das novas tecnologias "projetou-se sobre o fenómeno criminal, pois se atendermos às suas duas vertentes, por um lado, a tecnologia pode ser, ela mesma, objeto de prática de crimes e, por outro lado, suscita e potencia novas formas criminais ou novas formas de praticar crimes". SIMAS – ***Op cit.*** p. 14.

[426] SIMAS – ***Op cit.*** p. 15.

[427] BARBOSA – ***Op cit.*** p. 8.

[428] "Em primeiro lugar surgem as formas tradicionais da atividade criminosa (como a fraude ou a falsificação) que utilizam agora a internet como meio de cometer crimes que já ocorriam no mundo físico. Os crimes são os mesmos, apenas o meio utilizado para os cometer é que é diferente. Uma segunda categoria consiste na publicação de conteúdos ilícitos, como materiais que incitam ao terrorismo, à violência, ao racismo e xenofobia ou ao abuso sexual de menores. Finalmente, a terceira forma de cibercrime considerada pela UE diz respeito a "crimes exclusivos das redes eletrónicas, que são crimes novos e abrangentes, de larga escala, desconhecidos na era pré-internet." Nesta tipologia, os criminosos atacam os sistemas de informação, ameaçando as infraestruturas de informação cruciais do Estado e, consequentemente, ameaçando diretamente os cidadãos." DIAS – ***Op cit.*** p. 66-67. e BARBOSA – ***Op cit.*** p. 9.

Registe-se igualmente que o cibercrime pode "adotar várias formas, passando o ciberespaço a ser tanto um meio como um fim para a prática de atos ilícitos"[429].

De igual forma, genericamente, as referidas ameaças "assumem um caráter transfronteiriço, o que associado à arquitetura da internet não permite um controlo centralizado das atividades *online*, uma vez que a troca de informações sobre padrões de ameaças, anomalias no tráfego de rede e incidentes em resolução é crucial para determinar as medidas apropriadas e aplicáveis para a defesa e a segurança"[430].

A referida evolução conduziu a um novo paradigma de sociedade, o qual se consubstancia numa sociedade global[431], sem fronteiras, e permanentemente interligada entre todos, bem como assume um papel vital na política[432].

Estes desenvolvimentos, "quer a nível de *hardware* quer a nível de *software*, nas redes de informação e comunicação têm produzido alterações no *modus vivendi* das sociedades a nível global", as quais têm aumentado a nossa dependência em relação às TIC[433].

Como consequência desta dependência, têm surgido novas formas de cometimento do crime, as quais são ainda mais graves do que a criminalidade "normal", bem como acarretam dificuldades acrescidas na identificação dos seus autores. Assim, aliado à "distância transnacional a que os crimes podem ser cometidos surge o anonimato e a dificuldade, dentro de um hiato de tempo considerado indispensável, para a recolha de prova digital"[434].

Deste modo, o cibercrime assume diversas formas de ser definido, considerando que abrange uma vasta gama de diferentes ataques e que não existe um consenso na literatura quanto à sua definição. De acordo com a *Symantec Corporation*[435], em 2013, um cibercrime pode ser "qualquer crime que é cometido através de um computador ou rede, ou dispo-

---

[429] MOREIRA, João – **O Impacto Do Ciberespaço Como Nova Dimensão Nos Conflitos.** Boletim Ensino. Investigação n.º 13. Lisboa: Instituto Universitário Militar, 2012. p. 41.

[430] Como Altford enfatiza, "a única medida razoável de eficácia é detetar a infiltração cibernética quando isso acontece". O mesmo autor observa ainda que, "quando descoberto, um incidente precisa ser relatado a outras entidades, incluindo não apenas os responsáveis pela mitigação, mas também às possíveis vítimas". Tradução livre do autor. TIKK, Eneken – **Comprehensive legal approach to cyber security.** Estonia: University of Tartu, Faculty of Law, 2011. Tese de Doutoramento. ISBN 978-9949-19-763-7. p. 113.

[431] A internet provocou uma revolução na história da humanidade, assumindo assim "uma grande relevância, quer através do setor económico criado pelo comércio eletrónico, quer através da influência cultural e educativa que ela exerce, abrindo cada vez mais possibilidades aos seus utilizadores". LEITÃO – ***Op cit.*** p. 172.

[432] VEIGA– ***Op cit.***

[433] Os sistemas informáticos conseguem alocar mais espaço de memória, numa relação proporcional de tamanho-espaço disponível, aliado à rapidez de execução de tarefas em simultâneo. Os dispositivos, de variada ordem, conseguem fazer com que estejamos contactáveis 24 horas por dia, sete dias por semana, de diversas formas, onde quer que nos encontremos. RAMOS, Armando – A novíssima diretiva relativa ao cibercrime. In SOUSA, Constança Urbano de (coord.) **O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes**. Lisboa: Ediual, 2014. ISBN: 9789898191618. p. 176.

[434] RAMOS – ***Op cit.*** 2014a. p. 177.

[435] Empresa que detém o *software* antivírus Norton.

sitivo de *hardware*. O computador ou dispositivo de *hardware* pode ser o agente do crime, facilitador ou alvo do crime"[436]. Na prática, pode ser definido como uma qualquer atividade criminosa, perpetrada através do ciberespaço ou da internet, a qual abrange como instrumentos ou alvos primordiais os computadores e os sistemas informáticos.

Em complemento, sublinhe-se que os "crimes informáticos incluem atividades criminosas que envolvem o uso da infraestrutura tecnológica da informática, tais como: falsidade informática, acesso ilegal (acesso não autorizado), intercetação ilegal (uso de técnicas de transmissão não públicas de dados de computador para fora do sistema de computadores), obstrução de dados (danos a dados no computador, deteriorização dos dados), interferência nos sistemas (interferência nos sistemas de computadores quanto a entrada de dados), uso indevido de equipamentos, falsificação de IP's e fraude eletrónica"[437].

Deste modo, o cibercrime assume um caráter "cada vez mais complexo e, agora, o que está na moda são os *ransomware*: são programas maliciosos que sequestram dados, encriptando-os e cobrando um montante – quase sempre elevado – para os devolver"[438].

O cibercrime encontra-se regulado na Convenção de Budapeste sobre Cibercrime, ou também apelidada de Convenção do Cibercrime. Esta Convenção[439]é um acordo assinado entre os vários EM pertencentes à UE, e não só[440], que "surgiu com o intuito de controlar, e regular, os vários crimes cometidos através de dados eletrónicos"[441].

A mesma entrou em vigor em 1 de julho de 2004, após ter sido aberta à adesão por Estados terceiros[442]. O seu principal objetivo passa pela "harmonização entre os vários países signatários, dos elementos relativos às infrações, do direito penal, respeitantes a crimes realizados através de meios eletrónicos"[443], isto é, a cibercriminalidade. De igual modo, consagra a "implementação de um sistema de cooperação internacional, para que as

---

[436] FERNANDES – ***Op cit.*** p. 14. e MENEZES – ***Op cit.*** p. 26.
[437] MENEZES – ***Op cit.*** p. 26.
[438] Em sentido figurado: imagine que chega a casa e que não consegue abrir a porta porque alguém mudou a fechadura. NUNES, Flávio – **Cibersegurança. "Estamos em guerra, meus senhores".** [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://observador.pt/2016/04/13/cibersegurancaestamosguerrameussenhores/.
[439] A convenção foi adotada pelo Comité de Ministros do Conselho da Europa na Sessão n.º 109 de 08 de Novembro de 2001. Só posteriormente, em 23 de Novembro do mesmo ano, foi aberta à assinatura em Budapeste, tendo entrado em vigor, em 01 de julho de 2004.
[440] Esta Convenção foi elaborada por um comité de peritos nacionais, congregados no Conselho da Europa e consiste num documento de Direito Internacional Público. Pese embora este documento tenha sido criado por iniciativa europeia, na Convenção de Budapeste, participaram vários outros países, tais como EUA, Japão, Canadá e África do Sul.
[441] ALMEIDA, Ivo – **A Prova Digital.** Lisboa: Universidade Autónoma de Lisboa, 2014. Dissertação de Mestrado. p. 40.
[442] RAMOS – ***Op cit.*** 2014a. p. 178.
[443] ALMEIDA – ***Op cit.*** p. 40.

infrações cometidas por meio de sistema informático tenham o acompanhamento, auxílio, e apoio dos demais Estados Membros"[444].

Esta Convenção surgiu da necessidade de regular o cibercrime. Para tal, no seu preâmbulo, na exposição de motivos, expõem-se "quatro fortes argumentos para a sua existência: 1.º aproximar o direito penal dos EM no domínio dos ataques contra os sistemas de informação, estabelecendo um conjunto de regras mínimas relativamente às infrações penais e às suas sanções; 2.º a utilização de *botnets*[445] para fins criminosos, que coloca em causa sistemas de informações de infraestruturas críticas da União, comprometendo a realização de uma sociedade de informação mais segura e de um espaço de liberdade, segurança e justiça; 3.º aumentar a eficácia dos pontos de contacto 24/7, responsáveis pela aplicação da lei nos EM; e, 4.º fazer face à falta de dados estatísticos sobre os ciberataques"[446].

Com efeito, a CBC foi "o primeiro tratado internacional a lidar com a internet e a criminalidade no ciberespaço, sendo o instrumento jurídico por excelência na política de cooperação internacional sobre o cibercrime"[447], no qual "estão previstas as definições comuns e proibições criminais, procedimentos e regras para garantir um processo legal simplificado de forma a facilitar a cooperação internacional no âmbito da cibersegurança e da ciberdefesa"[448]. Assim, aos Estados signatários da CBC é exigido que[449]:

(1) Decretemos delitos e as sanções nos termos previstos "nas suas leis nacionais para quatro categorias de crimes informáticos – fraude e falsificação, pornografia infantil, violação

---

[444] *Ibidem*.

[445] "Na própria exposição de motivos encontramos a definição de *botnet*. Assim, "o termo «*botnet*» designa uma rede de computadores que foram infetados por *software* maligno (vírus informáticos). Esta rede de computadores «sequestrados» («*zombies*») pode ser ativada para executar ações específicas, como atacar sistemas de informação (*ciberataques*). Estes «*zombies*» podem ser controlados – frequentemente sem o conhecimento dos utilizadores dos computadores «sequestrados» – por outro computador, igualmente conhecido como «centro de comando e de controlo». As pessoas que controlam este centro fazem parte dos infratores, já que utilizam os computadores «sequestrados» para lançar ataques contra os sistemas de informação. É muito difícil localizar os autores da infração, dado que os computadores que formam o «*botnet*» e realizam o ataque podem encontrar-se num local diferente daquele em que se encontra o infrator." [Consult. 10 Out. 2019]. Disponível em WWW:<URL: http://new.eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX%3A32013L0040&qid=1377248567337.

[446] RAMOS – ***Op cit.*** 2014a. p. 184.

[447] Além dos EM, fizeram parte da CBC com o estatuto de "observadores", a África do Sul, o Canadá, os EUA e o Japão. Apesar da condição de "observador" na CBC, estes desempenharam um papel crucial tanto na formulação como nas negociações deste documento, sobretudo pela sua vasta experiência nas questões relacionadas com a defesa do ciberespaço e tratamento dos cibercrimes. VATIS, M. – The Council of Europe Convention on Cybercrime. In: **National Research Council of The National Academies, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.** Washington D.C.: The National Academies Press, 2010. p. 207-223.

[448] SCHJOLBERG, S. – **Computer-related offences.** Conselho da Europa, 2004. [Consult. 10 Out. 2018]. Disponível em WWW:<URL: http://cybercrimelaw.net/documents/Strasbourg.pdf.

[449] ARCHICK, K. – **Cybercrime: The Council of Europe Convention.** Budapeste: Conselho da Europa, 2005.

de direitos de autor e violações de segurança, tais como *hacking*, intercetação ilegal de dados e interferências do sistema que possam comprometer a integridade e a disponibilidade da rede. Os signatários também devem promulgar leis que estabeleçam a jurisdição sobre as infrações cometidas nos seus territórios, navios registrados ou aeronaves, ou pelos seus nacionais no exterior"[450].

(2) Definam "procedimentos nacionais para detetar, investigar e processar crimes informáticos e recolher provas eletrónicas de qualquer delito cometido no ciberespaço. Tais procedimentos incluem a preservação acelerada de dados armazenados em computador ou comunicações eletrónicas, busca no sistema e interceção de dados em tempo real. As partes na CBC devem garantir as condições e salvaguardas necessárias para proteger os direitos humanos e o princípio da proporcionalidade"[451].

(3) Constituam um "rápido e eficaz sistema de cooperação internacional. A CBC considera que os crimes cibernéticos são delitos extraditáveis e permite que as autoridades responsáveis pela aplicação da lei de um Estado recolham provas informáticas noutro Estado. Também exige a criação de uma rede de contactos para prestar assistência (vinte e quatro horas, sete dias por semana) imediata a investigações transfronteiriças"[452].

Para além da Convenção de Budapeste sobre o Cibercrime, esta tipologia criminal encontra-se regulada igualmente em Portugal na Constituição da República Portuguesa (art.ºs 27.º n.º 1, 61.º e 62.º) e na Lei do Cibercrime, bem como ao nível internacional na Convenção Europeia dos Direitos do Homem (art.º 5.º) e Carta dos Direitos Fundamentais da UE (art.ºs 6.º, 16.º e 17.º), no sentido de dar proteção jurídica à liberdade de utilização dos sistemas informáticos e das redes sem interferências alheias.[453]

De igual modo, não podemos olvidar que o "fenómeno crescente da globalização e os acelerados avanços tecnológicos (…) impulsionaram novas dinâmicas de mudança, nos contextos políticos, social e económico a nível mundial"[454]. Na prática, vivemos numa "época de mudança de paradigma social em que a vida das sociedades modernas se transfere do real para o virtual"[455].

---

[450] ALMEIDA, Cláudia – A Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço. In **III Seminário IDN Jovem.** N.º 30. Lisboa: IDN, [s.d.]. p. 277.
[451] ALMEIDA – **Op cit.** p. 278.
[452] *Ibidem*.
[453] MASSENO, Manuel **– Os Crimes contra Sistemas Informaticos e Redes Abertas.** Slide 8.
[454] AMARAL, Sandra – **O Papel dos Serviços de Informações no Combate ao Ciberterrorismo: o Caso Português.** Lisboa: Academia Militar, 2014. Dissertação de Mestrado. p. 2.
[455] AMARAL – ***Op cit.*** p. 4.

Deste modo, a Lei n.º 72/2015[456], de 20 de julho, que define os objetivos, prioridades e orientações de política criminal para o biénio de 2015-2017, em cumprimento da Lei n.º 17/2006, de 23 de maio, que aprova a Lei-Quadro da Política Criminal, veio expor que o terrorismo e a cibercriminalidade são crime de prevenção prioritária, nos termos respetivamente do art.º 2.ºa) e m). O art.º 3.º considera os mesmos como crimes de investigação prioritária, de acordo com as alíneas a) e h), respetivamente.

Por outro lado, atentemos que o atual Código de Justiça Militar[457] vem igualmente definir que são crimes contra a segurança do Estado os seguintes: inteligências com o estrangeiro (art.ºs 28.º e 30.º); prática de atos adequados a provocar guerra (art.º 29.º); espionagem (art.º 34.º); e violação de segredo de Estado (art.ºs 33.º e 316.º do CP).

Não obstante toda a referida previsão legal, consideramos que a mesma apresenta algumas fragilidades, a saber: visão tradicional de cibercrime – atividade motivada por razões estritamente económicas, não contendo soluções adequadas para dar resposta a ataques de motivação política; e dificuldades legais de desenvolvimento de atividades de vigilância da rede, para determinar a origem dos ataques e dar-lhes resposta – atividades reservadas a Orgãos de Polícia Criminal, sob estritas formalidades que tornavam obsoleto o recurso às mesmas.[458]

Outro aspeto pertinente prende-se com a falta de uma uniformização das normas penais e processuais penais a nível internacional, no que se refere aos crimes informáticos ou cometidos através de meios informáticos. Se "nos crimes tradicionais a prática de um ilícito penal poderia ser investigada no decurso do tempo e circunscrito a um espaço mais confinado, tal não sucede com os cometidos através das redes de informação e comunicação. Efetivamente, no que à recolha de prova digital diz respeito, por exemplo, o tempo corre a desfavor das autoridades que investigam pois os registos informáticos podem ser apagados de vez, numa fração de segundos"[459]. Neste contexto é que surgiu a CBC, na tentativa de se obter uma uniformização da legislação internacional, mormente a nível europeu, sobre a temática do cibercrime.

Por outro lado, relembremos que a "guerra cibernética tem como objetivo os sistemas que estão relacionados com a infraestrutura nacional de energia (eletricidade, petróleo e

[456] Lei n.º 72/2015. **Diário da República I Série.** N.º 139 (20-07-2015). p. 4909-4911.
[457] Lei n.º 100/2003, de 15 de Novembro, com a retificação n.º 02/2004, de 03 de janeiro.
[458] CASIMIRO, Sofia – **Curso de Mestrado em Guerra de Informação / *Competitive Intelligence* da Academia Militar**. 2015.
[459] Por outro lado, a transnacionalidade ou ocultação da identidade são outros dos fatores a ter em conta na investigação deste tipo de delitos. RAMOS – ***Op cit.*** 2014a. p. 177.

gás), o sistema financeiro e a infraestrutura social (transportes e outros serviços públicos), contribuindo para a diminuição da capacidade de defesa e de reação do Estado"[460].

Com efeito, o surgimento do ciberespaço acarretou a necessidade de se garantir a segurança dos que a ele recorrem ou dele dependem, tendo-se para tal definido os seguintes pilares de ação no âmbito da cibersegurança[461]:

a) Cibercrime – A crescente utilização do ciberespaço originou um "aproveitamento ilícito das novas potencialidades por ele conferidas. A atividade criminosa no ciberespaço pode surgir de diversas formas e nos mais variados contextos. Com o objetivo de se poder regular legislativamente estas práticas ilícitas, sentiu-se necessidade de estabelecer categorias nas quais se pudessem integrar as diferentes tipologias de ação criminosa neste espaço"[462].
b) Hacktivismo – Primitivamente esta "prática foi desenvolvida por especialistas que tentavam encontram falhas nos sistemas, seguida de uma fase em que o interesse era o de criar algo novo"[463]. Posteriormente, o Hacktivismo atingiu uma "expressão de atividades de índole criminosa que vão desde a pirataria ao desenvolvimento e implantação de *malware*"[464]; existem assim "quatro tipos de atividades desenvolvidas por *hackers*, que servem para as agrupar pelas suas caraterísticas: *hackers*[465], *phreakers*[466], *crackers*[467], *cypherpunks*[468] ou criptoanarquistas[469],,[470].

---

[460] Desta forma, observamos que a guerra cibernética está presente nos campos estratégicos, tático e operacional, desenvolvendo assim ações próprias do espaço cibernético. MENEZES – ***Op cit.*** p. 26.
[461] MILITÃO, Octávio – **Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional.** Lisboa: Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa, 2014. Dissertação de Mestrado. p. 26.
[462] *Ibidem*.
[463] "O termo *hacker* surgiu na década de 50 no MIT e referia-se àquele que de forma engenhosa encontrava uma solução não óbvia mas de certa forma elegante para um problema complexo. Esta expressão remetia para especialistas, para os programadores que, com o intuito de ajudar no desenvolvimento do ciberespaço, tentavam encontrar falhas nos sistemas, procurando corrigi-los ou encontrar algo novo a ser criado. Contudo, sobretudo devido ao surgimento do cibercrime, o termo *hacker* adquiriu nos últimos anos um significado pejorativo, começando a ser utilizado pelos *media* para designar os indivíduos que cometem atos ilícitos com recurso a meios informáticos. Atualmente, esta atividade atingiu uma expressão de índole criminosa que vai desde a pirataria ao desenvolvimento e implantação de *malware* (programas maliciosos), considerando-se agora *hacker* o indivíduo disponível e capaz de penetrar, explorar ou contornar barreiras de segurança para atingir um qualquer fim. O hacktivismo resulta assim do conjunto de atividades levadas a cabo por indivíduos que, aproveitando-se das vulnerabilidades do ciberespaço, desenvolvem atividades ilícitas, com o objetivo de prejudicar esses sistemas." MILITÃO – ***Op cit.*** p. 97. e BARBOSA – ***Op cit.*** p. 9.
[464] SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos – **Cyberwar – O Fenómeno, as Tecnologias e os Atores.** Lisboa: FCA, 2008.
[465] Normalmente são intrusos de diversos sistemas informáticos que criam e libertam *malware*.
[466] Praticam burlas e intrusões unicamente em redes de comunicações.
[467] A atividades destes *hackers* é removerem as proteções a determinados programas para que estes se tornem acessíveis por todos.
[468] Cfr. ASSANGE, Julian – **Cypherpunks. Liberdade e o futuro da internet.** Lisboa: Editempo Editorial, 2013.

c) Ciberespionagem – Esta "metodologia de ação é perentoriamente utilizada por Estados como forma de prevenirem ataques e potenciarem o seu crescimento económico, através da realização de ataques que procuram recolher informações que promovam um reconhecido poder estratégico"[471].

d) Ciberterrorismo – O "ciberterrorismo surge da união entre a prática do terrorismo e o imenso espaço do ciberespaço. O ciberterrorismo é uma prática ambicionada pois permite uma facilidade de ação e dispersão só alcançáveis neste meio. A estrutura da internet é semelhante à das novas redes de terrorismo[472], em rede e transnacional na sua ação e metodologia de ataque"[473].

Considerando o já exposto, refira-se que o cibercrime é um "problema que ultrapassa as fronteiras físicas, e por essa razão, devem-se concatenar meios, a nível mundial, para combatê-lo de forma eficaz"[474].

Deste modo, verifica-se um aumento da "preocupação com as questões que o ciberespaço levanta e, concomitantemente, com o agudizar das querelas com este relacionadas, [o que] deu origem a que a 10 de Fevereiro de 2016 a OTAN e a UE firmassem um acordo histórico com o intuito de combater o cibercrime e outras ameaças híbridas"[475]. Tal, demonstra a "profunda necessidade de criar estruturas, tanto a nível nacional como internacional, que estejam interligadas entre si e que funcionem como uma rede exclusiva de prevenção do cibercrime, muito como as equipas especializadas no combate à cibercriminalidade fora do ciberespaço"[476]. Com efeito, evidencia-se a "existência de organismos de pre-

---

[469] Especialistas em criptografia que desenvolvem métodos de proteção de comunicações ou ações maliciosas no ciberespaço.

[470] MILITÃO – ***Op cit.*** p. 27.

[471] PEREIRA, Júlio – Cibersegurança – O Papel do Sistema de Informações da República Portuguesa. In **Segurança e Defesa.** Maio-Agosto 2012. Lisboa: Diário de Bordo, 2012. e MILITÃO – ***Op cit.*** p. 28.

[472] Cfr. NOVAIS, Rui – Media e (Ciber)Terrorismo. In **Cibersegurança**. N.º 133. Lisboa: Nação e Defesa – Instituto de Defesa Nacional, 2012.

[473] MILITÃO – ***Op cit.*** p. 28-29.

[474] Conforme o disposto no art.º 20.º da Lei n.º 109/2009, de 15 de setembro, "as autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico, de um crime". Esta ideia também está patente no n.º 1 do art.º 25.º da Convenção sobre o Cibercrime, aprovada em Resolução da Assembleia da República N.º 88/2009, de 15 de setembro, segundo a qual os Estados deverão estabelecer relações de cooperação e conceder mutuamente o mais amplo auxílio possível para efeitos de investigação ou de procedimento relativos a infrações penais relacionadas com sistemas e dados informáticos, ou para efeitos de recolha de provas sob a forma eletrónica de uma infração penal." LEITE – ***Op cit.*** p. 12.

[475] "Ou seja, a NATO e a UE decidiram tomar medidas conjuntas, de modo a que as equipas de ambas as instituições possam dar uma resposta mais eficaz em caso de emergência. Para que tal seja concretizável, ficou acordado a criação de um quadro estruturado que facilite a troca de informações e a partilha de práticas mais avançadas."LEITE – ***Op cit.*** p. 13.

[476] "Com a exigência da criação de um Centro Nacional de Cibersegurança, a UE deu o mote para que este reúna as áreas militares e civis numa nova perspetiva de abordagem à estrutura regular de segurança e defesa,

venção de práticas ciberterroristas, de monitorização da prática de ciberespionagem e de equipas prontas para agir em caso de ciberguerra"[477].

De seguida, iremos procurar refletir um pouco sobre o ordenamento jurídico nacional, em particular, no que se refere aos principais normativos legais que regulam esta temática do Cibercrime e, consequentemente, da prova digital, a saber: o Código de Processo Penal; a Lei n.º 32/2008, de 17 de julho, que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas; e a LC.

Comecemos então pela Lei n.º 32/2008, de 17 de julho, a qual no seu art.º 4.ºvem preconizar que a conservação e preservação dos dados deve existir durante um ano.

Este normativo jurídico vem também definir a competência das autoridades judiciárias e dos OPC's quanto à preservação dos dados informáticos, bem como se estende quanto à pesquisa destes, e mesmo à sua apreensão. Explica-nos o mesmo diploma que as entidades competentes têm o dever de cooperação com as entidades competentes estrangeiras quando do mesmo modo, se tratar de crimes em que envolva a pesquisa, análise, apreensão, preservação de dados informáticos e especialmente recolha de prova. Todas estas manobras de investigação, seja de investigação no âmbito interno, ou de cooperação com entidades estrangeiras, devem, e estão ao abrigo da Lei, respeitando por sua vez o acordo com as normas sobre transferência de dados pessoais, as quais debruçam especial atenção, ao tratamento de dados pessoais, salvaguardando que este processo se deve realizar de forma transparente e no estrito respeito pela reserva da vida privada.[478]

De igual modo, vamos agora abordar a Lei do Cibercrime (Lei n.º 109/2009[479], de 15 de setembro), a qual estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico.[480]

Assim, a LC no âmbito do direito penal material tipificou seis crimes informáticos em sentido estrito: a falsidade informática (art.º 3.º), o dano relativo a programas ou outros dados informáticos (art.º 4.º), a sabotagem informática (art.º 5.º), o acesso ilegítimo

abrangendo o domínio cibernético. Deste modo, com a existência de um centro especializado poder-se-á, com mais facilidade e rapidez, responder aos problemas levantados pelos potenciais ataques ao ciberespaço, minimizando os danos diretos e colaterais." LEITE – ***Op cit.*** p. 17.

[477] Não foi ainda criada uma autoridade que, em última análise, detenha o controlo de todas as outras ou que simplesmente faça o papel de mediador e que proporcione uma maior conexão entre as mesmas.

[478] ALMEIDA – ***Op cit.*** p. 38.

[479] Adaptação da Convenção sobre o Cibercrime do Conselho da Europa (Convenção de Budapeste) e transposição da Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação. A Lei 109/2009, de 15 de setembro, teve por base a Lei n.º 109/91, de 17 de agosto, designada de Lei da Criminalidade Informática.

[480] MENEZES – ***Op cit.*** p. 39.

(art.º6.º), a interceção ilegítima (art.º 7.º) e a reprodução ilegítima de programa protegido (art.º 8.º). A grande evolução desta Lei é ao nível processual e da cooperação internacional. Ao nível processual é vital a adoção de "eficazes disposições processuais específicas porque estamos perante crimes específicos que destinam ao fracasso a aplicação de procedimentos tradicionais"[481]. Estas disposições processuais são fundamentais para "agilizar a investigação e a punição do cibercrime"[482], ao mesmo tempo que são "aplicadas a qualquer infração penal cometida por meio de um sistema informático e à recolha de prova em suporte eletrónico de qualquer infração penal"[483].

A Lei do Cibercrime assume como novidades as seguintes: redefinição e atualização das normas penais aplicáveis na área do cibercrime; criação de medidas processuais que viabilizem a obtenção e recolha de dados para afins de investigação criminal, através da criação de regimes próprios de preservação e meios de obtenção de prova relacionados com dados informáticos (art.º 12º a 15º) e da criação de especialidades quanto à apreensão de dados informáticos, correio eletrónico e registo de comunicações de natureza semelhante[484] (art.º 15º a 17º[485]); alargamento dos regimes jurídicos de interceções de comunicações e de ações encobertas (art.º 15º e 16º); e implementação de normas específicas relativas à cooperação internacional em matéria penal.[486]

Neste contexto, aproveitamos para dar a conhecer uma definição relativa aos crimes cibernéticos, os quais podem ser definidos como os "atos dirigidos contra um sistema informático, tendo como subespécies os atos contra o computador e atos contra os dados

---

[481] DIAS – ***Op cit.*** p. 84.
[482] *Ibidem*.
[483] *Ibidem*.
[484] "Pedro Verdelho, antes da revisão do CPP de 2007 defendia esta equiparação, argumentando que "não existem normas específicas que regulamentem a obtenção e utilização, como meio de prova, das mensagens de correio eletrónico", remetendo então para a norma da integração de lacunas (art.º 4.º do CPP), para defender que a expressão contida no art.º 179.º n.º 4 ("qualquer outra correspondência") não se ficaria apenas pelo correio tradicional." VERDELHO, Pedro – A obtenção da prova no ambiente digital. In **Revista do Ministério Público.** N.º 99. Ano 25. Julho-Setembro 2004. p. 122. Rogério Bravo vai ainda mais longe, ao afirmar que "a vingar esta corrente de pensamento [no sentido de o correio eletrónico dever ser tratado como correspondência tradicional], não restarão dúvidas de que em consequência, também terão de cair sob a mesma categoria de "correspondência" as mensagens de e para telemóveis, ou qualquer outro tipo de mensagens escritas com destino a terminais de comunicações, nomeadamente, os chamados SMS's e MMS's." BRAVO, Rogério – Da não equiparação do correio electrónico ao conceito tradicional de correspondência por carta. In **Revista Polícia e Justiça**. III Série. N.º 7. Janeiro-Junho 2008. Coimbra: Coimbra Editora, 2008. p. 2. GONÇALVES, João – A prova digital em 2017 – Reflexões sobre algumas insuficiências processuais e dificuldades da investigação In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 57. Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2017. p. 27.
[485] "O art.º 17.º da lei do cibercrime vem regular a apreensão do correio eletrónico, onde se prevê que o juiz possa autorizar ou ordenar a apreensão dos emails que possam ser importantes para a descoberta da verdade." GONÇALVES – ***Op cit.*** p. 28.
[486] VIEIRA, Rui – **A Prova Digital.** Lisboa, Universidade Autónoma de Lisboa, 2015. Pós-graduação em Ciências Criminais.

ou programas de computador"[487]. De igual modo, podem ser os "atos cometidos por intermédio de um sistema de informação[488] e estão incluídas infrações contra o património, as infrações contra a liberdade individual e as infrações contra a propriedade imaterial"[489].

Nesta perspetiva, e considerando a dependência mundial desta sociedade que cresce e está permanentemente interligada e em rede, urge "defender os nossos sistemas e infraestruturas vitais contra o ataque de cibercriminosos e ao mesmo tempo promover a confiança em transações eletrónicas, para promoveras trocas, o comércio, as relações bancárias, a telemedicina, a administração pública eletrónica e outras aplicações eletrónicas"[490].

Deste modo, destaca-se a necessidade de uma correta aplicação da lei penal no ciberespaço, considerando-se esta como "o conjunto de regras e normas do direito referentes ao limite de aplicação da lei penal no ciberespaço"[491].

Neste prisma, cada Estado, no "exercício das suas funções ou atividades de soberania, possui a legitimidade para delimitar a amplitude do poder para punir e agregar ao conjunto de princípios referentes a aplicação da lei penal", uma vez que este "possui um poder punitivo de legitimidade própria em exercer uma coação penal perante o agente que pratica o delito e perante os demais Estados", o qual consiste num "pressuposto material necessário da sentença penal, visto que só cabe exercitar a coação penal quando corresponde ação submetida ao próprio poder punitivo".[492]

Face ao exposto, constatamos que as caraterísticas apresentadas pelo cibercrime levam a que seja difícil conseguir efetuar a sua prevenção, investigação, repressão e puni-

---

[487] MENEZES – ***Op cit.*** p. 40.

[488] "A informação é um recurso que tem valor essencial para as organizações, incluindo-se nesta aceção os Estados: é um valor decisivo e fundamental nos dias em que vivemos e assume um aspeto relevante na segurança e defesa das nações. Qualquer interrupção de serviço público, utilização indevida de informação classificada ou destruição de dados de cariz importante pode pôr em causa a confiança dos cidadãos e os interesses – e até a própria soberania – dos Estados." Assim, um "sistema de informação é considerado seguro se reunir as seguintes características: confidencialidade, no sentido de permitir o acesso apenas a utilizadores autorizados; integridade, ou seja, a garantia de que a informação é a correta; disponibilidade, o que significa a possibilidade de utilizar a informação quando ela é necessária." VAZ – ***Op cit.*** p. 40.

[489] MENEZES – ***Op cit.*** p. 40.

[490] Declarações de Kofi Annan, à data Secretário-Geral das Nações Unidas, em 17 de maio de 2006, aquando das comemorações do dia Mundial da Sociedade da Informação, que nesse ano foi dedicado à promoção da cibersegurança. VAZ – ***Op cit.*** p. 41.

[491] MENEZES – ***Op cit.*** p. 58.

[492] "Portanto, cada Estado soberano tem a competência de traçar os limites próprios do poder punitivo, porém, respeitando as regras estabelecidas pelo direito Internacional. Devido aos limites impostos ao poder punitivo de cada Estado é necessária a análise da eficácia da soberania de jurisdição penal frente aos delitos que possuem uma chamada "matriz internacional". Desta forma, ao tratarmos da problemática do conflito da jurisdição como critério da aplicabilidade da lei penal no espaço, torna-se imperativo à análise dos quatro princípios básicos: princípio da territorialidade, princípio da personalidade, princípio da defesa e o princípio da universalidade." MENEZES – ***Op cit.*** p. 58.

ção, levando a que haja um estudo e uma preocupação cada vez maiores, no sentido de reduzir o sentimento de insegurança que o mesmo potencia.

Com efeito, a problemática da investigação do cibercrime deverá ser considerada tendo por base a premissa de que o desenvolvimento do cibercrime num ambiente virtualizado, como é o caso do ciberespaço, gera uma dificuldade adicional na sua investigação.

Assim, o combate ao cibercrime terá de ser encarado num contexto de proteção do ciberespaço, isto é, verifica-se a necessidade do desenvolvimento de legislação que se constitua como prevenção geral, de forma a prevenir e a sancionar as condutas julgadas lesivas para o desenvolvimento da sociedade da informação e do comércio eletrónico. Ao mesmo tempo, este quadro legislativo terá como necessidade a manutenção do regular funcionamento das infraestruturas vitais para a sociedade, especialmente as infraestruturas críticas da informação e das comunicações. Por último, e não menos importante, terá como objetivo fundamental a repressão dos comportamentos singulares ou coletivos que sejam levados a cabo contra ou por intermédio das TIC.Com o rápido desenvolvimento das TIC, a "informação tem-se tornado cada vez mais um importante recurso na vida das pessoas e, particularmente, nas atividades operacionais e estratégicas das instituições e organizações, [o qual passou a ter a capacidade de] (…) marcar a diferença entre o sucesso e o insucesso no âmbito da sociedade da informação"[493].

Neste particular, a existência de legislação difusa e ainda pouco consolidada, dificulta a investigação deste tipo de criminalidade, bem como ainda se depara com os problemas inerentes à preservação da cadeia de prova e a sua valoração como prova em sede de julgamento. Particularizando um pouco melhor esta problemática, refira-se que esta criminalidade assume um caráter transnacional, o que implica uma necessidade ainda maior de harmonização da legislação penal, com os inerentes instrumentos em matéria de direito processual penal e a cooperação judiciária internacional[494].

Assim, são facilmente identificáveis as inerentes dificuldades de prevenção, investigação, recolha de prova e punição. Tal acontece devido à maior facilidade do cometimento do crime neste paradigma do ciberespaço, sendo que muito do mesmo nem sequer chega ao conhecimento oficial das autoridades, uma vez que se desenvolve na *DarkWeb*.

---

[493] LAGARES – ***Op cit.*** p. 15.

[494] Alguns exemplos desta necessária cooperação são os casos de: preservação e divulgação de dados de tráfego a pedido das autoridades competentes, a busca e apreensão de dados informáticos armazenados, a recolha em tempo real de dados de tráfego, a interceção do conteúdo de comunicações, entre outros.

Para o combate a este tipo de criminalidade, bem como propiciar uma melhor investigação, terá de se verificar uma intervenção, a nosso ver, nos seguintes domínios: a adequação de legislação à realidade do cibercrime; a conceção de uma metodologia uniforme e partilhada por todos os atores que combatem este crime, tanto ao nível nacional como internacional; interoperabilidade dos sistemas de partilha de informação e de preservação da cadeia de prova; uma maior celeridade na cooperação das entidades internacionais; e uma partilha efetiva, atual e sem restrições de toda a informação disponível, seja ao nível nacional ou internacional.

Com efeito, a prova digital é indissociável do cibercrime, a qual pode definir-se como sendo "qualquer tipo de informação, com valor probatório, armazenada (em qualquer dispositivo de armazenamento digital) ou transmitida (em sistemas e redes informáticas ou redes de comunicações eletrónicas, privadas ou publicamente acessíveis), sob a forma binária ou digital"[495].

A prova digital pode ainda ser definida como toda e qualquer "informação passível de ser obtida ou extraída de um dispositivo eletrónico (local, virtual ou remoto) ou de uma rede de comunicações, razão pela qual esta prova digital, para além de ser admissível, deve ser também autêntica, precisa e concreta"[496].

Desta feita, a prova digital, tal como qualquer outra prova, tem de "reter o seu valor probatório, para que este seja suscetível de ser valorado pelo julgador, e crie a sua convicção de veracidade do facto"[497]. Com efeito, "a diferença que se encontra entre esta e as demais provas, é a caraterística do formato digital. Sendo assim, pode esta ser armazenada ou transmitida também no meio digital, seja num computador, ou qualquer dispositivo capaz de conservar com segurança a prova"[498].

Como vimos acima, atualmente temos uma lógica legislativa que tem primado pela dispersão dos normativos legais, considerando que continua a manter "em vigor três diplomas legais diferentes para regular aspetos parcelares da mesma realidade concreta. Esta situação gera uma assimetria, uma incoerência das soluções legais e, sobretudo, dificulta a sua aplicação com sucesso prático"[499]. A resolução desta situação deverá passar

[495] RODRIGUES, Benjamim – **Direito Penal Parte Especial.** Tomo I. Coimbra: Direito Penal Informático Digital, 2009. p. 722. e ALMEIDA – ***Op cit.*** p. 26-27.
[496] RAMOS, Armando – **A Prova Digital em Processo Penal.** Lisboa: Chiado Editora, 2014. Versão eBook. p. 97.
[497] *Ibidem*.
[498] *Ibidem*.
[499] Para um maior desenvolvimento desta problemática consultar CORREIA, João – Prova Digital: as leis que temos e as que devíamos ter. In: **Revista do Ministério Público.** N.º 139. Julho-Setembro 2014. p. 29-59.

pela codificação ou a junção num único normativo legal, o qual deverá ser "coerente, global e, cientificamente, sustentável"[500].

A prova digital atualmente constitui o cerne da generalidade dos nossos processos penais, estando a mesma regulada em três diplomas legais já referidos: o CPP; a Lei n.º 32/2008, de 17 de julho; e, ainda, a LC[501]. De igual modo, encontra-se regulada: na CBC; no Código Penal[502]; na Lei 52/2003, de 22 de agosto (Lei de Combate ao Terrorismo); e na recente Lei 58/2019, de 08 de agosto (Lei da Proteção de Dados Pessoais).

A prova digital apresenta caraterísticas únicas em relação à prova tradicional, pelo que se afigura como vital a sua rápida recolha (em tempo real ou tempo útil), de modo a evitar a sua destruição. Esta apresenta ainda como caraterísticas: temporária, instável, frágil, alterável, imaterial, complexa ou codificada/encriptada, espacialmente dispersa, dinâmica, mutável, manipulável, dependente de terceiros, "extremamente volátil, facilmente contaminável, difícil percurso criminoso, transnacional, e exige intervenção imediata"[503].

Face ao exposto, impõe-se uma alta tecnicidade do investigador e do ambiente em que se produz a investigação: métodos de recolha (*live forensic* ou *post-mortem forensic*); equipamentos (equipamento esterilizado, embalagem adequada); formação e treino especializado dos OPC's, autoridades judiciárias, advogados e restantes operadores jurídicos e civis envolvidos (para evitar erros comuns).

De igual modo, exige-se uma multidisciplinaridade: técnicas de investigação criminal de crimes cibernéticos têm de se apoiar noutras ciências (engenharia informática, a psicologia criminal), a fim de precaver a interceção, a interpretação e a conservação dos dados.

A ação de recolha da prova digital não deve alterar a prova digital original, devendo tal ser feito com recurso a algoritmos de *hashing* credíveis e reconhecidos. De igual modo, só deve aceder à prova digital original quem for tecnicamente competente e apenas quando necessário: integridade da prova e garantia de autenticidade.

---

[500] CORREIA – ***Op cit.*** p. 29.

[501] Esta trilogia, para além de acentuar o atual paradigma da descodificação e de negar a desejável centralidade normativa do CPP, contribui para a assimetria, para a incoerência das soluções legais e, sobretudo, para o seu indesejável e nefasto insucesso prático. A prova digital – essencial no mundo hodierno – continua mergulhada num verdadeiro pântano prático e, sobretudo, normativo, que só poderá ser superado mediante uma intervenção legislativa coerente, global e, cientificamente, sustentável. CORREIA – ***Op cit.*** p. 30.

[502] Contém disposições sobre crimes informáticos e crimes cometidos com recurso à informática.

[503] VIEIRA, Rui – **A Prova Digital.** Lisboa, Universidade Autónoma de Lisboa, 2015. Pós-graduação em Ciências Criminais.

A atividade relacionada com a recolha[504], acesso, armazenamento ou transferência da prova digital, deve ser documentada e preservada para análise e auditoria, a fim de garantir a custódia da prova[505], bem como estar ciente que quem estiver na posse da prova digital é responsável pelas ações tomadas sobre ela, nomeadamente, o registo de todas as ações efetuadas sobre os dispositivos e fontes de recolha.

Por outro lado, é necessário atentar ao ciclo de vida da prova digital: 1. reunião; 2. identificação; 3. armazenamento; 4. preservação; 5. transporte; e 6. apresentação.[506]

Na realização dos exames periciais sobre cópias da prova digital, deveremos ter a garantia da integridade probatória em sede de inquérito criminal ou cível, considerando as inerentes caraterísticas legais da prova digital, a saber: admissível[507]; autêntica[508]; precisa[509]; e completa[510].

As TIC acarretaram novos desafios no que se refere à investigação judiciária, em particular aos meios de prova, com o aparecimento da prova digital. Neste sentido, importa referir que importantes ferramentas ficaram ao dispor da investigação, sendo "um dos desafios do legislador arranjar um adequado compromisso entre, por um lado, a segurança dos cidadãos, a realização da justiça e a descoberta da verdade (que podem ser reforçadas com os novos meios à disposição dos OPC) e, por outro lado, a salvaguarda dos direitos, liberdades e garantias e a proteção dos dados pessoais e da privacidade"[511].

A prova digital opera em pleno ambiente digital, o qual "não tem um significado jurídico propriamente dito mas cuja noção tem a utilidade de estabelecer uma fronteira compreensível entre o contexto físico (materializado numa realidade apreensível pelos sen-

---

[504] Princípios na recolha da prova: continuar a aplicar todos os princípios forenses já existentes; cuidados acrescidos para não alterar a prova; treino Especializado; documentação aturada da custódia da prova. VIEIRA – ***Op cit.***

[505] A prova é difícil de manter intacta, pelo que, deve ser manuseada com extremo cuidado. De igual modo, a mesma está sujeita ao livre arbítrio da apreciação da prova pelos juízes e, em alguns casos, à falta de formação dos órgãos de justiça. *Ibidem*.

[506] *Ibidem*.

[507] Estreita observância da lei e dos princípios legais por parte do responsável da investigação – art.º 32.º n.º 8 e 34.º da CRP, e art.º 126.º do CPP.

[508] Prova gerada e registada na cena ou lugar de um crime e não sofreu qualquer alteração – a volatilidade e capacidade de manipulação são grandes.

[509] Ligada à credibilidade da fonte e à possibilidade de a mesma ser verificada – a fiabilidade da prova está ligada à forma de organização de um sistema ou rede, ganhando em confiança sempre que se optimizarem os seguintes fatores: organização do armazenamento, política de *backup's* e sincronização de dados.

[510] O conjunto de atividades geradas pelo sistema informático terá de assegurar a correlação entre os diversos registos e dados informáticos armazenados, sem que se perca a integridade, sincronização e significado.

[511] GONÇALVES – ***Op cit.*** p. 1.

tidos) e o contexto digital (imaterial e impercetível aos sentidos sem a mediação de sinais elétricos)"[512].

Contudo, a prova digital constitui uma categoria ainda não totalmente autonomizada, pelo que é "necessário recorrer à analogia ou à interpretação extensiva de normas referentes a outras categorias probatórias, nomeadamente por força do art.º 189.º do CPP[513]„[514].

Nesta perspetiva, Rogério Bravo refere que, na prática, "aquilo que de facto se protege no Direito Penal da Criminalidade Informática é, por um lado, a disponibilidade, a confidencialidade, o não repúdio e a integridade dos dados, que interpretados, constituem informação; por outro lado, protege-se a disponibilidade, a confidencialidade e a integridade do processamento electrónico, nas diferentes fases de integração tecnológica que permite a acumulação, o armazenamento e a transmissão desses dados"[515].

Porém, a permanente necessidade de preservação da prova, associada à própria natureza da prova digital dificulta a sua exata regulação, uma vez que a prova digital tem "uma natureza intrinsecamente efémera, instável e facilmente alterável, sendo que esta mutabilidade dificulta a preservação da integridade da prova bem como o fundamental não repúdio da mesma. [Assim,] a prova digital, devido a esta fragilidade, tem de ser tratada de forma cuidada, na medida em que um mero descuido poderá efetivamente torná-la inutilizada"[516].

Deste modo, afigura-se necessário legislar no âmbito da investigação[517] desta nova realidade criminal, considerando que a prova digital se encontra atualmente espalhada na maioria das "vertentes do nosso quotidiano: telemóveis, *tablets*, computadores, máquinas fotográficas, sistemas de videovigilância, gravadores de áudio, e até em automóveis e em

---

[512] O "conceito de ambiente digital engloba apenas os dados informáticos que, de algum modo, são criados, processados, armazenados e são identificáveis em sistemas informáticos, de modo a que podem ser acedidos directa ou remotamente. Será, portanto, aquilo que jaz em forma binária e que é virtualmente acessível a um utilizador através da mediação de tecnologias de informação". RAMALHO, David – **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Almedina, 2017. p. 37.

[513] "Art.º 189.º/CPP: (Extensão) (após a alteração pela Lei n.º 48/2007, de 29 de agosto)
1 - O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes. 2 - A obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do art.º 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo".

[514] GONÇALVES – ***Op cit.*** p. 7.

[515] BRAVO, Rogério – **As Tecnologias de Informação e a Compressão dos Direitos, Liberdades e Garantias: os efeitos das regras "10/10" e "1/1"**. 2012. p. 1.

[516] GONÇALVES – ***Op cit.*** p. 9.

[517] Para aproveitamento das autoridades policiais dos novos poderosos meios de obtenção de prova e para limitar o acesso e utilização dos mesmos de modo a não ferir nucleares direitos, liberdades e garantias.

eletrodomésticos a podemos encontrar"[518], entre outros. Sublinhe-se que "todos estes aparelhos contêm fontes diferentes de prova, cada qual exigindo um processo diferente de recolha de prova, de acordo com a própria ENISA[519]„[520].

Assim, a recolha da prova digital assume uma especial complexidade[521], devendo a mesma obedecer aos cinco princípios estabelecidos pela ENISA: o princípio da integridade dos dados[522], o princípio da cadeia de custódia da prova (que se traduz no processo de preservação da integridade da prova digital)[523], o princípio do apoio especializado[524], o princípio do treino apropriado[525], e o princípio da legalidade[526].

Por outro lado, em Portugal não está definido uma modelo de recolha, preservação e apresentação da prova digital, pelo que "a ciência forense digital portuguesa se pode basear, grosso modo, no modelo proposto pelo *National Institute for Standards and Technology* (NIST), baseado em quatro etapas: a recolha (*collection*), o exame (*examination*), a análise (*analysis*) e o relatório (*reporting*)"[527].

Considerando o supracitado, verifica-se que a prova digital se depara com os problemas inerentes à preservação da cadeia de prova e a sua valoração como prova, em sede de julgamento. Assim, assume uma capital importância o papel da forças de segurança na recolha e preservação da prova digital.

Neste particular, iremos então abordar o contributo da Guarda Nacional Republicana[528] (GNR) para a recolha e preservação da prova digital.

---

[518] GONÇALVES – ***Op cit.*** p. 15.
[519] A ENISA refere que "existem inúmeras fontes de evidência digital e cada uma exige um processo diferente para recolher essas evidências, bem como diferentes ferramentas e métodos para este efeito. Não são apenas os computadores pessoais, *laptops*, telemóveis ou a internet que fornecem fontes de evidência digital; qualquer peça de tecnologia digital que processa ou armazena dados digitais pode ser usada para cometer um crime. O dispositivo e as informações que ele contém podem armazenar evidências digitais relevantes para provar ou refutar uma ofensa suspeita". Tradução livre do autor. ENISA – **Electronic evidence – a basic guide for First Responders. Good practice material for CERT first responders.** United Kingdom: Northumbria University, 2014. ISBN 978-92-9204-111-3. [Consult. 27 Mar. 2019]. Disponível em WWW:<URL: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders. p. 4.
[520] GONÇALVES – ***Op cit.*** p. 16.
[521] Recordemos que "existem preocupações que vão desde o momento da chegada ao local do crime à avaliação e apresentação da prova, e que se alastram ao risco de erro por força de influências externas promovidas pelos agentes do crime, pelas próprias vítimas ou ainda pelos investigadores que recolhem a prova." GONÇALVES – ***Op cit.*** p. 17.
[522] ENISA – ***Op cit.*** p. 6.
[523] ENISA – ***Op cit.*** p. 7.
[524] *Ibidem*.
[525] ENISA – ***Op cit.*** p. 8.
[526] *Ibidem*.
[527] ENISA – ***Op cit.*** p. 7. e GONÇALVES – ***Op cit.*** p. 18.
[528] A GNR tem por missão, no "âmbito dos sistemas nacionais de segurança e proteção, assegurar a legalidade democrática, garantir a segurança interna e os direitos dos cidadãos, bem como colaborar na execução da

Pela sua natureza e polivalência, a GNR encontra o seu posicionamento institucional no conjunto das forças militares e das FSS, sendo a única força de segurança com natureza e organização militares, caraterizando-se como uma força militar de segurança, bem como um OPC de competência genérica no âmbito da investigação criminal.

Assim, a GNR constitui-se assim como uma Instituição charneira, entre as FA e as forças policiais e serviços de segurança[529].

Com efeito, refiram-se algumas das competências da GNR previstas no art.º 3.º da Lei n.º 63/2007, de 06 de novembro, que podem ocorrer no ciberespaço: "garantir as condições de segurança que permitam o exercício dos direitos e liberdades e o respeito pelas garantias dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de direito; garantir a ordem e a tranquilidade públicas e a segurança e a proteção das pessoas e dos bens; prevenir a criminalidade em geral, em coordenação com as demais FSS; desenvolver as ações de investigação criminal e contraordenacional que lhes sejam atribuídas por lei, delegadas pelas autoridades judiciárias ou solicitadas pelas autoridades administrativas; manter a vigilância e a proteção de pontos sensíveis, nomeadamente infraestruturas rodoviárias, ferroviárias, aeroportuárias, (…) edifícios públicos e outras instalações críticas"[530].

De igual modo, "analisando os órgãos superiores de comando e direção[531] da Guarda, identificamos nas Direções do Comando Operacional um conjunto de competências que também podem ser prosseguidas no ciberespaço"[532], a saber:

---

política de defesa nacional, nos termos da Constituição e da lei", nos termos do art.º 1º, nº 2, da LOGNR. Deste modo, trata-se de uma "missão extensa, multifacetada e exercida em todo o território nacional (continuidade temporal e territorial), no âmbito dos sistemas nacionais de segurança e proteção, bem como na execução da política de defesa nacional". MACHADO, Paulo – **O Papel da GNR no Contexto da Cibersegurança Nacional.** Lisboa: Instituto de Estudos Superiores Militares, 2015. Trabalho de Investigação Individual do CEMC – 2014/15. p. 33.

[529] Em situação de normalidade, a Guarda executa fundamentalmente as típicas missões policiais, mas não só, porque decorre da sua missão, a atribuição de missões militares no âmbito da defesa nacional, em cooperação com as FA e é aqui que reside a grande diferença para com as Polícias. Em situações de estado de emergência ou de sítio, devido à sua natureza, organização e à formação dos seus militares, apresenta-se como a força mais indicada para atuar em situações problemáticas e de transição entre as Polícias e as FA. Já em caso de guerra, pela sua natureza militar e pelo dispositivo de quadrícula, que ocupa todo o território nacional, pode, isoladamente ou em complemento, desempenhar um leque muito alargado de missões das FA. De igual forma, pode cobrir todo o espetro de missões no âmbito das denominadas OOTW ("*Operations Other Than War*" – Operações para além da Guerra), desde a fase de imposição à de manutenção, em complemento das FA, com principal relevância para as fases pós-conflito, e ainda, as tarefas de polícia em substituição das polícias civis, nas fases posteriores e antes de alcançada a segurança e a estabilidade suficientes para que aquelas possam atuar. *Ibidem*.

[530] MACHADO – ***Op cit.*** p. 33-34.

[531] Conforme n.º 3 do art.º 21º da Lei n.º 63/2007 e Decreto Regulamentar n.º 19/2008 de 27 de novembro.

[532] MACHADO – ***Op cit.*** p. 35.

- Direção de Operações: elaborar e difundir diretivas sobre prevenção criminal, policiamento comunitário e programas especiais, nomeadamente, no âmbito (…) do apoio e proteção de menores, idosos e outros grupos especialmente vulneráveis ou de risco;
- Direção de Informações: proceder à pesquisa, análise e difusão de notícias e informações com interesse para a missão da Guarda; realizar as adequadas averiguações de segurança em caso de quebra ou comprometimento de segurança de informação, nos termos da legislação em vigor;
- Direção de Investigação Criminal: proceder ao tratamento da informação criminal em coordenação com a Direção de Informações e assegurar a difusão de notícias e elementos de informação; acompanhar a evolução da criminalidade e o surgimento de novas táticas e técnicas aplicáveis à investigação criminal;
- Direção de Comunicações e Sistemas de Informações: assegurar a direção, coordenação, controlo, gestão e execução das atividades da Guarda em matéria de (…) sistemas e tecnologias da informação, segurança da informação (…); assegurar, em coordenação com as entidades nacionais responsáveis, o (…) controlo das atividades da Guarda no domínio específico dos sistemas criptográficos e de segurança da informação.

Os incidentes e ataques maliciosos que têm como alvo infraestruturas de informação dos governos, instituições públicas e privadas, empresas e cidadãos têm registado um aumento. De igual modo, saliente-se a dificuldade em "reconstituir qualquer percurso criminal entre os diferentes agentes delituosos, em virtude dos atos serem praticados em diversos pontos do ciberespaço, sentindo-se os infratores protegidos pelo anonimato que este domínio lhes proporciona"[533].

Neste contexto global foi definida a Diretiva Estratégica[534] do Comandante-Geral da Guarda para o período compreendido entre 2015 e 2020, definindo como um dos objetivos estratégicos da Guarda para este horizonte temporal, o incremento da "capacidade de atuação no mundo ciber, garantindo uma resposta integrada da instituição ao fenómeno da cibercriminalidade no mundo real e virtual"[535].

---

[533] MACHADO – ***Op cit.*** p. 1.

[534] Constitui-se como um documento enformador do planeamento e programação em termos de estratégia institucional.

[535] Conforme GUARDA NACIONAL REPUBLICANA – **Estratégia da Guarda 2020 – Uma Estratégia de Futuro**. [Em Linha]. [Consult. 03 Jan. 2018]. Disponível em WWW:<URL:http://www.gnr.pt/portal/internet/dcrp/EG2020/eg2020.swf. Neste contexto várias congéneres da GNR têm vindo a criar valências de prevenção (*Cyberpolicing*), tendo constituídas unidades policiais especializadas neste domínio (ex: *Grupo Delitos Telemáticos* em Espanha, *Département Cybercriminalité* em França, ou o *Reparto Indagini Techniche* em Itália). MACHADO – ***Op cit.*** p. 35-36.

Uma vez que "os fenómenos criminais ligados ao ciberespaço estão a evoluir e a crescer exponencialmente, sendo os seus efeitos pouco compreendidos ou percecionados pelas diversas entidades públicas ou privadas e pelos próprios cidadãos"[536], refira-se que no âmbito da atuação das FSS a "partilha da informação e a cooperação constituem elementos decisivos na prevenção e no combate ao diferente espetro das ciberameaças"[537].

Para responder a estes desafios, e à inerente responsabilidade no âmbito das capacidades de prevenção e investigação no ambiente digital, a GNR, através da Direção de Investigação Criminal, criou duas Secções com competências no âmbito da investigação do Cibercrime e da recolha de prova digital. Neste sentido, à Repartição de Análise Forense Digital compete contribuir para a execução das competências dos órgãos superiores no âmbito da vertente de investigação criminal – criminalística, através da:

- Secção de Recolha de Prova Digital, a qual: realiza estudos, pareceres, exames e perícias referentes à recolha de prova em qualquer dispositivo, sistema ou infraestrutura no âmbito das TIC; efetua análise forense no âmbito da criptografia e de estenagrofia; e outras que, direta ou indiretamente, estejam relacionadas com a investigação criminal, lhe sejam acometidas;
- Secção de Investigação de Ciberincidentes, no sentido de: apoiar os órgãos da Guarda no âmbito da cibersegurança com atribuições nesta tarefa: garantir ações de investigação dos crimes tradicionais que se perpetuam com recurso às TIC, os relativos à proteção de dados pessoais ou os que estejam relacionados com conteúdos ilícitos; e outras que, direta ou indiretamente relacionadas com a investigação criminal, lhe sejam acometidas.

De seguida, iremos analisar dois crimes que ocorrem bastante no ciberespaço: o crime de furto de identidade *online* e o crime de "acesso indevido".

O crime de furto de identidade[538]*online* consiste na "usurpação e uso ilegítimo de identidade alheia através da apropriação dos dados pessoais, em ambiente digital, com o

[536] MACHADO – ***Op cit.*** p. 36.
[537] Deste modo, o grau de ameaça subjacente e a necessidade urgente de prevenir e reprimir os seus efeitos implica um correto dimensionamento, a geração e a reorganização de competências e valências de entidades que têm responsabilidades na área da segurança, como é o caso da Guarda. MACHADO – ***Op cit.*** p. 36.
[538]Para entendermos com mais clareza o sentido de "identidade" recorreremos em primeira instância à Declaração Universal dos Direitos do Homem (DUDH) onde, segundo o seu art.º 6º, se confere a todos os indivíduos o "direito ao reconhecimento da sua personalidade jurídica. Não se reconhece expressamente o direito à identidade, mas reconhece-se a identidade como um direito da personalidade (portanto, como um direito do indivíduo, enquanto pessoa singular, física). Remetendo-nos para o ordenamento jurídico nacional, mais concretamente para a Lei Fundamental, temos no seu art.º 16º (âmbito e sentido dos direitos fundamentais) uma remissão clara para a DUDH.

objetivo de praticar fraude quase sempre tendo em vista a obtenção ilícita de vantagens e benefícios financeiros e ou levar a efeito outras atividades criminosas[539],,[540].

Nesta tipologia criminal podem ser furtados "diversos tipos de dados pessoais como o nome, o sexo, a naturalidade ou a data de nascimento, bem como outros que lhes estejam relacionados tais como a morada da vítima, os números de cartão do cidadão e de identificação fiscal, informações relacionadas com os cartões de crédito, a carta de condução ou, ainda, outros documentos pessoais e fotografias"[541]. Deste modo, os "autores do furto de identidade digital apropriam-se das informações alheias para diversos fins ilícitos"[542].

O tema do furto de identidade *online* tem merecido particular atenção por parte da indústria de segurança informática, a qual tem vindo a dedicar um interesse crescente pelo mesmo, ao ponto de algumas empresas evidenciarem essa problemática através de *slogans* e campanhas.[543]

O crime de "acesso indevido", previsto e punido no art.º 47.º da Lei da Proteção de Dados Pessoais (Lei n.º 58/2019, de 08 de agosto), está normalmente associado, mas também confundido, com o crime de acesso ilegítimo, previsto e punido no art.º 6.º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro). Todavia, o legislador ao dar-lhes epígrafes diferentes pretendeu "não só individualizar o acesso a dados pessoais, bem como configurar a hipótese de um concurso real de normas, ou seja: o acesso indevido não é uma ação contra o sistema, mas sim contra os dados que ali se encontrem, podendo-se configurar que o acesso indevido aos dados ocorra como consequência e em concurso com um acesso ilegítimo ao sistema"[544].

Após analisarmos sumariamente estas duas tipologias criminais, vamos agora dissecar um pouco melhor a recolha da prova.

Neste particular, importa que, antes de mais, a organização esteja preparada para "que computadores ou suportes digitais pertencentes ou presentes na empresa possam ter

---

[539] Este tipo de furto pode consistir numa atividade criminosa conduzida por pessoa isolada ou, na sua forma mais grave, estar relacionada com o crime organizado ou mesmo para suportar a prática de atos terroristas.
[540] SANTOS, Paulo – **Furto de Identidade *On-line*.** [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://portalciber.gnr.local/wordpress/index.php/2015/12/21/furto-de-identidade-on-line/.
[541] *Ibidem*.
[542] "Os mais usuais são: efetuar a abertura, a consulta ou a transferência de saldos de contas bancárias; requerer cartões de crédito e ou débito; celebrar contratos fraudulentos; solicitar empréstimos ou créditos bancários para consumo de bens ou serviços; obter cuidados médicos ou medicamentos prescritos; obter certidões de nascimento ou de casamento, tendo em vista receber benefícios, pensões ou prestações diversas de natureza social; usurpar a identidade em sites, blogues, fora ou redes sociais." *Ibidem*.
[543] TEIXEIRA, Paulo – **O fenómeno do *Phishing*. Enquadramento jurídico-penal**. Lisboa: Universidade Autónoma de Lisboa, 2013. Dissertação de Mestrado. p. 25.
[544] MARQUES, Pedro – **Informática Forense. Recolha e preservação da prova digital** Lisboa: Universidade Católica Portuguesa. Faculdade de Engenharia, 2013. Dissertação de Mestrado. p. 112-113.

de ser apreendidos pelas autoridades para serem examinados pela prática de crimes tão diversos como a violência doméstica, o furto de identidade, as burlas, as falsificações, o tráfico de estupefacientes, os homicídios, o abuso sexual de crianças, as ameaças, as difamações ou o jogo ilegal"[545].

Deste modo, a "preservação de prova digital implica responsabilidades críticas adicionais, tais como: utilização de um conjunto de técnicas que não alterem ou destruam a prova; as análises dos sistemas devem ser realizados por pessoas treinadas e habilitadas para o efeito e que possam em sede judicial testemunhar sobre os passos realizados"[546].

Face ao exposto, importa agora sistematizar algumas ideias principais, a saber:

1) As "insuficiências do regime legal relativo à prova digital são reais e manifestam-se em artigos como o art.º 179.º do CPP [apreensão de correspondência], que simbolicamente representa as omissões que ainda persistem relativamente às TIC na lei portuguesa"[547].

2) "As três leis principais que contêm normas processuais relativas à prova digital (CPP, Lei do Cibercrime e Lei n.º 32/2008) não se encontram perfeitamente delimitadas, sendo por vezes complexa a perceção do regime a aplicar, podendo-se possivelmente pensar numa solução legislativa mais simples e clara"[548].

3) Em relação aos "métodos ocultos de investigação criminal em ambiente digital, a utilização dos mesmos tem como inevitável consequência a restrição de direitos fundamentais: por esse mesmo motivo, nunca são retirados da equação os métodos proibidos de prova nem tão-pouco os princípios a respeitar sempre que está em causa a restrição de Direitos, Liberdades e Garantias (DLG's)"[549].

---

[545] Devemos ainda ter em atenção aquelas "situações em que a empresa é a própria vítima, como em casos de acessos ilegítimos ou indevidos a informação, situações que envolvam *ransomware* ou relacionadas com o desempenho dos seus colaboradores, em que embora se entenda não haver motivos de participação criminal às autoridades, há que estar preparado para recolher de forma eficaz a prova digital, que pode vir a ser de capital importância num processo cível ou de trabalho." Por outro lado, "a preparação, quer de responsáveis e operacionais de sistemas informáticos, quer de juristas que têm de lidar com a prova digital, apresenta insuficiências, o que tem levado muitas vezes à anulação de provas em tribunal por inadmissibilidade legal, no caso dos primeiros ou à não verificação da integridade legal da prova por desconhecimento das suas nuances técnicas, no caso dos segundos." MARQUES – ***Op cit.*** p. 114.

[546] MARQUES – ***Op cit.*** p. 120.

[547] Estabelece o n.º 1 deste artigo que "sob pena de nulidade, o juiz pode autorizar ou ordenar, por despacho, a apreensão, mesmo nas estações de correios e de telecomunicações, de cartas, encomendas, valores, telegramas ou qualquer outra correspondência (…)". Ora, atendendo à disseminação da utilização de correspondência eletrónica, afigura-se incompreensível a persistente omissão relativamente à mesma e a necessidade de ainda se ter de recorrer, quanto muito, a uma interpretação extensiva da parte final do trecho citado." GONÇALVES – ***Op cit.*** p. 32-33.

[548] Conforme demonstrado no citado acórdão do Tribunal da Relação de Évora de 06.01.2015, que remete as situações relacionadas com os dados especificamente previstos no art.º 4.º da Lei 32/2008 para o regime processual deste diploma, e todos os outros dados que aí não estejam previstos para o regime contido na Lei n.º 109/2009. GONÇALVES – ***Op cit.*** p. 33.

[549] *Ibidem*.

4) Já "as buscas *online*[550] são poderosas ferramentas de investigação que não devem ser negligenciadas pelo legislador: apesar de terem ínsita uma compressão dos DLG's não negligenciável, o potencial de investigação é demasiado importante para ser ignorado e não se procurar chegar a uma nova solução legislativa"[551].

5) Relativamente aos "dados de tráfego e dos dados de localização[552], deveria o legislador fazer uma clarificação, de modo a que não haja espaço para a subsistência de posições doutrinárias que recusem a admissibilidade desta prova digital devido à falta de tipicidade destes meios de obtenção de prova"[553].

6) Quanto à prova digital importará estudar o seu alargamento para além do direito criminal. "A verdade é que se trata de uma ferramenta poderosa na descoberta material da verdade, a qual poderia ser fundamental para que se ajudasse a fazer justiça noutros tribunais que não [só] os criminais"[554].

7) A Diretiva NIS "poderá e deverá ter, acima de tudo, um papel determinante no reforço dos poderes da CERT[555] (serviço integrante do CNCS português encarregue de coordenar a resposta a incidentes de cibersegurança envolvendo o ciberespaço nacional)"[556].

8) As principais dificuldades da investigação da cibercriminalidade assentam no seguinte: "interpretação dos diplomas *à la carte*; transnacionalidade; cooperação internacional morosa ou não existente; evolução técnica versus adaptação jurídica"[557].

9) Em relação aos desafios do cibercrime poderemos elencar: "dificuldades acrescidas na responsabilização por atuações ilícitas em rede: facilidade de reprodução (com rapidez e sem perda de qualidade); rapidez de transmissão; poucos rastos dos atos praticados (ex. reprodução); e maior anonimato"[558].

2.2. O Terrorismo e o Ciberterrorismo

[550] As mesmas correspondem a um método oculto de investigação criminal.
[551] GONÇALVES – ***Op cit.*** p. 33.
[552] Como é o caso da tecnologia GPS.
[553] GONÇALVES – ***Op cit.*** p. 34.
[554] GONÇALVES – ***Op cit.*** p. 35.
[555] "Por um lado, pode e deve o CNCS ver aumentados os seus poderes de articulação entre as CSIRT nacionais ou internacionais, devendo haver igualmente uma consolidação e um reforço das suas funções de coordenação operacional e de autoridade nacional em matéria de cibersegurança relativamente às entidades públicas e às infraestruturas críticas nacionais Por outro lado, (…) [deveremos] permitir o alargamento dos poderes de acesso a tráfico de dados, por parte do CNCS, no âmbito da cibersegurança e do ciberterrorismo – o que, a acontecer, produzirá inevitavelmente alguns efeitos ao nível da prova digital." *Ibidem*.
[556] *Ibidem*.
[557] VIEIRA – ***Op cit.***
[558] CASIMIRO, Sofia – **Curso de Mestrado em Guerra de Informação / *Competitive Intelligence* da Academia Militar.** 2015. Slide 8.

2.2.1. O Terrorismo

Antes de mais importa aqui referir que o terrorismo surge como um atentado à segurança internacional, o qual iremos sumariamente estudar de seguida.

Deste modo, recuemos ao século XX, onde o Realismo veio consagrar a "conceção de segurança legada por Maquiavel, Hobbes e Clausewitz: o Estado soberano, ator unitário, como objeto e provedor da segurança; a segurança nacional[559] como principal nível da segurança; a sociedade internacional anárquica[560] de onde decorrem as ameaças, como ambiente em que se desenvolve a problemática da segurança dos Estados; o conflito interestadual como tipo dominante de conflito; a força militar e a diplomacia como meios usados pelo Estado para providenciar pela sua segurança; a política de defesa como política de segurança político-militar em relação a ameaças externas; e a separação entre segurança externa e segurança interna"[561].

Historicamente, o conceito de segurança aparece especialmente associado à ideia de segurança militar e do Estado[562]. Neste modelo, a "segurança nacional assume-se como um sistema de sistemas, assentes em conceitos estratégicos autonomizados mas sistematicamente interdependentes e ancorados numa filosofia de ação em que a complementaridade e a subsidiariedade são elementos essenciais"[563].

A segurança pode ser definida como a ausência de uma ameaça à estabilidade e soberania do Estado. Deste modo, devido à evolução da sociedade humana e à globalização, o conceito de segurança sofreu alterações significativas, sendo que algumas dessas transformações resultaram da presença do fenómeno da violência, que se traduz, sobretudo, num sentimento de insegurança, o qual é causado pela perceção de insegurança e pelo medo.

Associado à insegurança e ao medo surgiu o fenómeno do terrorismo, o qual entrou no nosso léxico com a Revolução Francesa de 1789, uma vez que, nos primeiros anos da Revolução, "os Governos tentavam impor a nova ordem, em grande parte, através da vio-

[559] Defesa da soberania, da integridade territorial, dos valores e dos interesses dos Estado.
[560] Descentralizada, competitiva, sem autoridade supra-estadual.
[561] BRANDÃO, Ana – As tendências Internacionais e a posição de Portugal. In **Actas.** I Congresso Internacional do OBSERVARE. Lisboa: Universidade Autónoma de Lisboa, 2011. p. 5.
[562] Esta alteração da natureza da segurança acontece no quadro complexo dos processos sociais, económicos, políticos e tecnológicos associados à globalização. No contexto de uma conflitualidade global, defende-se a ideia de se estar perante um novo paradigma de segurança, emergente nestas últimas duas décadas.
[563] LOURENÇO, Nelson – As Novas Fronteiras da Segurança – Segurança Nacional, Globalização e Modernidade. In **Segurança e Defesa.** N.º 31 – fevereiro-junho 2015. Lisboa. p. 26.

lência. Como resultado, o primeiro significado da palavra "Terrorismo", conforme registado pela *Académie Française* em 1798, foi de sistema ou regra de terror"[564].

Todavia, a sua definição não é linear, considerando que o conceito de terrorismo "deriva da diversidade de motivos que mobilizam os terroristas, dos fins que prosseguem e dos métodos que empregam, combinado com o facto de que o terrorista, que alguns denunciam, é o lutador pela liberdade que outros prezam"[565].

Com efeito, o ataque terrorista define-se por ser efetuado de "surpresa, pela sua violência extrema e por ter como alvo preferencial a população, locais ou infraestruturas de utilização massiva, havendo enorme probabilidade de ocorrência de um elevado número de vítimas. Provoca o terror, o pânico e o medo constante, obrigando as pessoas a viverem em permanente sobressalto, condicionando o seu normal modo de vida"[566].

Com o passar dos anos, o conceito inicial de terrorismo foi-se adaptando à nossa realidade, pelo que se considera a alteração do seu paradigma na década de 1990, a partir do momento em que Osama Bin Laden se tornou líder do movimento islâmico, a *Al-Qaeda*.

Esta alteração alavancou-se nas declarações públicas deste novo líder, o qual evidenciava "uma mistura de extremismo religioso, desprezo para com os atuais regimes árabes, hostilidade face ao domínio dos EUA e insensibilidade quanto aos efeitos que as suas ações provocavam"[567]. Deste modo, germinava um "novo tipo de movimento terrorista, com uma determinada causa, organizado em rede, que não se limitava a um único Estado e cujos apoiantes estavam dispostos a cometer suicídio para destruir os seus adversários"[568].

Assim, o terrorismo assenta num "método onde através da adoção de medidas violentas, sejam estas de caráter físico ou psicológico, praticada por indivíduos provenientes de grupos políticos, ou ideológicos, que visa por em causa a ordem estabelecida, e que estes mesmos actos se podem manifestar através de ataques a indivíduos, a grupos de indivíduos, ou ainda e numa escala mais abrangente, a um governo ou uma população"[569].

Deste modo, constate-se que o terrorismo, enquanto crime internacional, pode assumir diferentes formas e manifestações. As suas atividades visam a destruição dos direitos

---

[564] VARINO, Alexandre – **Terrorismo: a interrupção de sistemas.** Lisboa: Instituto de Estudos Superiores Militares, 2012. Trabalho de Investigação Individual do CEMC – 2011/12. p. 6.
[565] *Ibidem*.
[566] *Ibidem*.
[567] VARINO – ***Op cit.*** p. 7.
[568] *Ibidem*.
[569] FERREIRA, Renato – Globalização e Segurança. Um mundo em mudança. In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 8 Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2015. p. 30.

humanos e das liberdades fundamentais. O mesmo pode ainda divergir quanto aos atos, os métodos e as práticas terroristas.

A ideia de incluir o terrorismo como um dos crimes mais graves que afetam a comunidade internacional encontra-se patente no projeto de Estatuto do TPI da Comissão de Direito Internacional de 1994[570].

Esta temática não foi, contudo e mais uma vez, abordada na Conferência de Revisão de Kampala de 2010. Indubitavelmente, a principal dificuldade prende-se com a ausência de uma definição jurídico-política universal consagrada numa convenção global sobre o terrorismo internacional, prescrevendo que os atos terroristas em grande escala constituem um crime internacional[571].

Com efeito, o terrorismo poderá ser compreendido como a "utilização ilegal de força ou de violência planeada contra pessoas ou património, na tentativa de coagir ou intimidar governos ou sociedades para atingir objetivos políticos, religiosos ou ideológicos"[572].

Segundo o Professor António Lara, o terrorismo "inclui todos os atentados e agressões que visam generalizar um dano de monta a um paciente previamente indefinido, anónimo ou indistinto. É relativamente irrelevante quem morre ou fica ferido, desde que morra ou fique ferida muita gente (…) também pode visar um alvo concreto que se quer pressionar, eliminar, chantagear, fazer desaparecer de cena ou condicionar de forma definitiva, com vista a alterar o paralelograma de forças ou o circunstancialismo político de uma determinada correlação vigente"[573].

Por outro lado, os ataques perpetrados no dia 11 de setembro de 2001 aos EUA tiveram o condão de mudar de forma perene o paradigma da segurança mundial.

Estes ataques impactaram na forma como a segurança passou a ser entendida mundialamente. Desta forma, a ameaça passou a assumir uma natureza transnacional, ditando "a investigação sobre a relação entre segurança interna e a segurança externa e sobre os atores estaduais como fontes de insegurança. Em sentido inverso, a resposta à ameaça, sig-

[570] A proposta da Comissão consistiu na integração de um artigo (o art.º 20.º) que contemplava, a par dos crimes de genocídio, de agressão, de violações graves das leis e costumes aplicáveis em conflitos armados e de crimes contra a humanidade, uma alínea específica, a alínea e), relativa aos "*treaty crimes*" nos quais se inseria o terrorismo.

[571] Vários autores frisam que atos de terrorismo internacional, como os ataques de 11 de setembro de 2001, poderiam ser considerados como crimes contra a humanidade de acordo com o art.º 7.º do Estatuto e julgados pelo TPI.

[572] Esta é a definição de Terrorismo da OTAN, expressa no MC 472. OLIVEIRA, Guerreiro – **Terrorismo Transnacional. Conhecer o Inimigo.** Lisboa: Instituto de Estudos Superiores Militares, 2008. Trabalho de Investigação Individual do CEMC – 2007/08. p. 4.

[573] LARA, António – **O Terrorismo e a Ideologia do Ocidente**. Coimbra: Edições Almedina, 2007. p. 44.

nificou o retorno do Realismo"[574], na perspetiva de adoção de "políticas que reforçam as fronteiras (físicas, biométricas e digitais) e o Estado como provedor de segurança, ataques territoriais, e segurança militar"[575].

Contudo, o terrorismo, assumindo diversas formas, ainda não atingiu uma definição consensual, embora possa expressar, *lato sensu*, um clima de medo e terror[576].

Depois dos atentados de 11 de setembro de 2001, os quais tiveram o seu foco na imprevisibilidade, o terrorismo deu mostras da sua vitalidade com os atentados de 2004 em Madrid[577], de 2005 em Londres ou de 2010 em Moscovo.

Se os ataques de 11 de setembro de 2001 relançaram a questão sobre atos terroristas em grande escala poderem constituir "crimes internacionais" e recair sob a alçada do TPI, presentemente podem-se enunciar diversos argumentos que fundamentam a consagração do terrorismo como crime da competência deste Tribunal. Os referidos ataques foram considerados pelo CS como uma ameaça à paz e segurança internacionais, através da Resolução n.º 1368, de 2001. Em várias Resoluções, este órgão reafirmou que o terrorismo em todas as suas formas e manifestações constitui uma das ameaças mais graves à paz e segurança internacionais, tendo a Estratégia Global de Combate ao Terrorismo da Assembleia Geral das NU de 2006 se referido a este fenómeno[578] nos mesmos termos[579].

Em complemento, sublinhe-se que os atentados de 11 de setembro de 2001 contribuíram para o aumento do sentimento de insegurança na ordem mundial. Como vimos, apesar de os EUA serem o principal alvo do terrorismo e, noutro patamar, o Reino Unido, a Espanha, a França ou a Rússia, certo é que nenhum lugar do mundo pode traduzir um sentimento de segurança absoluto, pois o novo paradigma do terrorismo, de natureza global e transnacional, assenta na incerteza e imprevisibilidade.

---

[574] BRANDÃO – ***Op cit.*** p. 10.
[575] *Ibidem*.
[576] Os fenómenos da criminalidade organizada e do terrorismo, embora concetualmente diferentes, mas inseridos numa ameaça transnacional, podem conduzir a um interessante debate sobre o esbatimento de fronteiras entre a Segurança e Defesa.
[577] "Depois do atentado contra as Torres Gémeas, um dos atos terroristas que mais afetou a atenção da opinião pública, não apenas espanhola, mas mundial, foi o que teve lugar em 11 de março de 2004, em Madrid, sempre tendo por objeto e finalidade, quebrar a relação de confiança entre a população e a estrutura governativa." MOREIRA, Adriano – A estratégia global contra o terrorismo. In **Jornal Público.** Ed. 01 de julho de 2014. p. 46.
[578] A sua gravidade é acentuada pelas diferentes e múltiplas formas e manifestações que assume perpetrado também por atores não estatais, grupos que recorrem a diferentes métodos e detêm diferentes motivações.
[579] Além disso, o princípio *nullum crimen sine lege* ao prever que nenhuma pessoa poderá ser criminalmente responsabilizada pela sua conduta quando esta não constitua, no momento que tiver lugar, um crime de competência do Tribunal (art.º 22.º), poderia significar que os autores de atos terroristas, a coberto deste princípio, permaneceriam impunes.

Deste modo, refira-se que o terrorismo é instrumental, ou seja, é um meio e não um objetivo final, servindo deste modo para influenciar a opinião pública, através do recurso sistemático ao terror, bem como pela indiscriminação das vítimas a atingir e pela violência utilizada, a fim de evidenciar a incapacidade do Estado para proteger os seus cidadãos e, de igual modo, criar um clima de medo que impeça o normal funcionamento da sociedade. Neste particular, é necessário sempre algum cuidado na análise das suas motivações ou objetivos a atingir, porque os seus propósitos nem sempre são imediatos ou evidentes.

Como tal, para conseguirmos ter uma visão mais abrangente sobre as diferentes tentativas de concetualização do terrorismo, devemos igualmente conhecer a perspetiva institucional do fenómeno vertida em diversos documentos oficiais, sejam eles: de caráter político, como no caso do Conselho da UE que entende o terrorismo como um "ato que, pela sua natureza ou pelo contexto em que for cometido, seja suscetível de afectar gravemente um País ou Organização Internacional (OI), quando o seu autor vise intimidar gravemente uma população ou constranger indevidamente os poderes públicos ou uma OI, a praticar ou abster-se de praticar qualquer ato, ou desestabilizar gravemente ou destruir as estruturas fundamentais políticas, constitucionais, económicas ou sociais de um País ou de uma OI"[580]; ou de âmbito da doutrina militar, como o caso da OTAN, que entende o terrorismo como uma "utilização ilegal de força ou de violência planeada contra pessoas ou património, na tentativa de coagir ou intimidar governos ou sociedades para atingir objectivos políticos, religiosos ou ideológicos"[581].

Já o ordenamento jurídico português, através da Lei 52/2003, de 22 de agosto[582], define o terrorismo como sendo "a atuação concertada de duas ou mais pessoas, que vise prejudicar a integridade e a independência nacionais, impedir, alterar ou subverter o funcionamento das instituições do Estado previstas na Constituição, forçar a autoridade pública a praticar um ato, a abster-se de o praticar ou a tolerar que se pratique, ou ainda intimidar certas pessoas, grupos de pessoas ou a população em geral, mediante diversas formas de crime: a) crime contra a vida, a integridade física ou a liberdade das pessoas; b) crime contra a segurança dos transportes e das comunicações, incluindo as informáticas, telegráficas, telefónicas, de rádio ou de televisão, instalações de serviços públicos ou destinadas

[580] Considerando (8) da Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho de 15 de março de 2017 relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho. [Em Linha]. [Consult. 24 Mar. 2020]. Disponível em WWW:<URL:https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32017L0541&from=EN.
[581] OLIVEIRA – ***Op cit.*** p. 4.
[582] Com as alterações introduzidas pela Lei n.º 16/2019, de 14 de Fevereiro.

ao abastecimento e satisfação de necessidades vitais da população; c) crime de produção dolosa de perigo comum, através de incêndio, explosão, (…); d) actos que destruam ou que impossibilitem o funcionamento (…) de meios ou vias de comunicação, instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população; e) investigação e desenvolvimento de armas biológicas ou químicas; f) crimes que impliquem o emprego de energia nuclear, armas de fogo, biológicas ou químicas, substâncias ou engenhos explosivos, meios incendiários de qualquer natureza, encomendas ou cartas armadilhadas, sempre que, pela sua natureza ou pelo contexto em que são cometidos, estes crimes sejam susceptíveis de afetar gravemente o Estado ou a população que se visa intimidar".

Ao nível académico, o terrorismo é analisado sobretudo no que diz respeito aos métodos, enquanto os políticos analisam o fenómeno no que toca aos seus objectivos e motivações. Do ponto de vista jurídico, apesar da definição supracitada, é de igual modo particularmente difícil alcançar um conceito de terrorismo, principalmente devido ao facto do terrorismo em si não ser um crime, pois é "apenas" um meio para atingir um fim, ou seja, todas as suas consequências – mortes, ferimentos, destruição, entre outras –, já estão devidamente tipificadas legalmente – homicídio, ofensas às integridade física, danos, entre outros –, tal como os seus atos preparatórios, nos casos em que a tentativa é criminalmente punível. Daqui deriva uma dificuldade que reside no facto de não haver meio de aferir objetivamente a intenção, motivação ou ideologia que serve de base ao ato terrorista.

Logo, como constatámos, a definição de terrorismo não é simples de conseguir, uma vez que, mais do que uma mera definição teórica ou ideológica, o próprio conceito encerra em si mesmo problemas de índole prática na sua prevenção e combate.

Todavia, alguns pontos comuns são identificáveis nas suas diferentes conceções: ameaça ou uso da violência (extrema) indiscriminada para atingir os seus objetivos políticos, os quais muitas vezes são camuflados em motivos sociais ou religiosos; imprevisibilidade das suas ações ou dos seus alvos; forma de conflito assimétrico e não convencional; o principal objetivo das suas ações é provocar o medo e o alarme; e, regra geral, é levado a cabo por grupos organizados que têm um propósito político[583] definido.

Por outro lado, podemos ainda constatar que o terrorismo possui motivações racionais, psicológicas, culturais, mas sobretudo políticas, sendo os seus objectivos demonstrar a vulnerabilidade e impotência do respetivo governo, atrair a simpatia da opinião pública

[583] As suas causas assentam, regra geral, no fundamentalismo religioso, no racismo, no desejo de independência nacional e/ou na revolta social.

pela escolha de alvos cuidadosamente selecionados que podem ser publicamente racionalizados, causar uma polarização e radicalização entre o público, levar o governo a tomar ações repressivas que provavelmente afetarão a sua legitimidade e credibilidade e apresentar os atos de violência para que pareçam atos heróicos. Por último, as suas consequências podem levar à morte, ao terror, à insegurança, à vingança, a represálias, à confusão, à incoerência e até ao desgoverno de um Estado.

Em complemento, importa igualmente referir outras ameaças que deverão ser consideradas, devido à sua pertinência e efeito destrutivo.

Neste sentido, a proliferação das Armas de Destruição Maciça (ADM) é potencialmente a maior ameaça à nossa segurança, apesar de os regimes instaurados pelos tratados internacionais e os mecanismos de controlo das exportações terem conseguido abrandar a proliferação das ADM e dos respetivos sistemas de lançamento. Contudo, o progresso das ciências biológicas pode vir a aumentar a potência das armas biológicas nos próximos anos; os ataques com produtos químicos e materiais radiológicos constituem também uma séria possibilidade. A disseminação da tecnologia em matéria de mísseis vem trazer igualmente um novo elemento de instabilidade[584].

No que respeita à criminalidade organizada, a grande parte das atividades dos grupos criminosos consiste no tráfico transfronteiriço de droga, mulheres, migrantes clandestinos e armas. A criminalidade organizada pode igualmente estar ligada ao terrorismo. O incremento da pirataria marítima representa uma nova dimensão da criminalidade organizada à qual deverá doravante ser consagrada maior atenção.

A conjugação de todos estes elementos será a principal ameaça a ter em conta, uma vez que o terrorismo está determinado a fazer uso da máxima violência, pelo que a disponibilidade de armas de destruição maciça à criminalidade organizada(inclui cibercriminalidade), acaba por provocar um enfraquecimento do sistema estatal e a privatização da força, o que poderá colocar-nos perante uma ameaça verdadeiramente radical.

Neste sentido podemos indicar assim um conjunto de ameaças que afetam a segurança internacional: proliferação de armas de destruição massiva, com eventual combinação de ameaça nuclear, química, biológica e radiológica; o terrorismo internacional; a criminalidade transnacional, violenta e organizada; os ciberataques, ciberterrorismo, e cibercrimi-

[584] O cenário mais assustador é o da aquisição de armas de destruição maciça por parte de grupos terroristas. Se tal acontecesse, um pequeno grupo teria capacidade para infligir danos a uma escala que antes se encontrava apenas ao alcance dos Estados e dos exércitos.

nalidade; os conflitos regionais; as crises humanitárias e desastres naturais; e a pirataria internacional, sobretudo marítima.

Recorde-se que, os atentados com maior impacto mundial, o caso do 11 de setembro e do 11 de março, evidenciaram uma série de fenómenos típicos de um mundo globalizado, que passa pela impotência dos aparelhos militares contra inimigos invisíveis, e relembra as estratégias políticas e económicas dos Estados no espaço global, destacando a mobilidade das empresas que atuam nestes cenários. Perante os atentados ocorridos em 2001 nos Estados Unidos, o terrorismo passaria a ser classificado como a maior ameaça à segurança internacional.

Com efeito, atualmente estamos perante um conjunto alargado de definições de terrorismo, sendo que a maioria se insere no conceito de Estado Falhado, em que a fragilidade do próprio Estado leva ao colapso das instituições estatais, instrumentos responsáveis pela segurança, bem-estar. Face a este conjunto de debilidades enumeradas anteriormente os Estados perdem a legitimidade do exercício do poder, associada a uma instabilidade político-social, acrescido do facto de perderem o monopólio do uso da força e da capacidade de controlarem o território nacional, gera o aumento da violência e o caos, o que favorece o aparecimento de redes de crime organizado e organizações terroristas.

Mais recentemente, a *Al-Qaeda*, alicerçada no ciberterrorismo, tem procurado aproveitar a tecnologia de rede para angariar seguidores e recrutar potenciais colaboradores, factualidade que aumenta ainda mais a imprevisibilidade de ataques terroristas.

Deste modo, os terroristas tendem a organizar-se em rede, uma vez que "as redes são mais eficientes a tratar informação"[585].

Neste particular, recorde-se que "as organizações hierárquicas, cujo êxito se deveu exatamente à necessidade de processar informação de um modo estruturado, têm enormes dificuldades no combate às atividades conduzidas por este tipo de atores do sistema internacional, apesar dos sucessos recentes na prevenção de alguns atentados"[586].

As atividades terroristas têm condicionado fortemente "a política internacional pelo desafio permanente que colocam à segurança internacional"[587], considerando que se tratam

---

[585] BAYLIS, John et al. – **Strategy in the Contemporary World.** 2nd Ed. Oxford: Oxford University Press, 2007. ISBN 978-0-19-928978-3. p. 207.

[586] "Até ao momento, o sucesso obtido pelas redes criminosas e terroristas deveu-se à sua capacidade de obter e explorar uma posição de superioridade informacional perante o sistema de Estados." EUGÉNIO, António – Porque é que os criminosos e os terroristas tendem a organizar-se em rede? In MOREIRA, Adriano; RAMALHO, Pinto (coord.) – **Estratégia.** Vol. XIX. Lisboa: Instituto Português da Conjuntura Estratégica, 2010. ISSN 1645-9083. p. 53.

[587] EUGÉNIO – ***Op cit.*** p. 54.

de atores não estatais e apátridas que desafiam os poderes dos Estados modernos, uma vez que "a rede constituída pelo sistema mundial contém, para além dos Estados, as redes criminosas e terroristas"[588].

Na questão das redes, refira-se que o que "carateriza uma rede para além da sua topologia (mais ou menos centrada, mais ou menos dirigida, mais ou menos ligada) é a sua simplicidade básica. Uma rede é um conjunto de nós e um conjunto de relações. Os nós podem não ter todos a mesma importância para o funcionamento da rede, havendo uns mais ligados (*hubs*) que outros"[589].

As organizações em rede são aproveitadas por redes criminosas e terroristas, as quais "apresentam como vantagens a flexibilidade, a agilidade e a adaptabilidade, de modo a transformar-se sob pressão e a obter o disfarce necessário às operações encobertas que tornam o seu desmembramento particularmente difícil"[590].

Neste sentido, as "organizações em rede procuram a resiliência pela mitigação do risco, tornando possível a regeneração de células destruídas. Por definição, não há centro de gravidade, do qual toda a organização dependa, que, uma vez atacado, faça perder a coerência da organização[591].

Com efeito, poderemos afirmar que o "recurso de organizações criminosas e terroristas a redes é um produto da maneira de agir típica da Era da Informação. Os propósitos destas organizações colocam desafios à rede de organizações políticas à escala mundial, as quais tendem a criar elas próprias antídotos que contrariam as primeiras"[592].

Nesta perspetiva, a UE estabeleceu um compromisso com os seus EM para "combater todas as formas de terrorismo por todos os meios ao seu alcance, em conformidade com

---

[588] *Ibidem*.
[589] A caraterização de um nó depende da natureza das ligações com outros nós, bem como das entidades interligadas. Um nó tanto pode ser uma bolsa de valores, na rede mundial de fluxos financeiros, como pode ser um conselho de ministros, na rede política que governa a UE. (CASTELLS, Manuel – **A Sociedade em rede.** 2ª Ed. São Paulo: UNESP, 1999. p. 498.) Assim, os nós podem revestir-se de formas organizacionais e de dimensões diversas. (STRATEGOR – **Política Global da Empresa: Estratégia, Estrutura, Decisão, Identidade.** 3ª Ed. Lisboa: Dom Quixote, 2000. ISBN 972-20-1706-3. p. 277.) EUGÉNIO – ***Op cit.*** p. 56.
[590] EUGÉNIO – ***Op cit.*** p. 60.
[591] Para Castells, "as caraterísticas das organizações bem sucedidas na economia informacional incluem: a capacidade para gerar conhecimentos e processar informações com eficiência; a capacidade de adaptação à geometria variável da economia global; a flexibilidade suficiente para transformar os seus meios tão rapidamente quanto mudam os objectivos sob o impacto da rápida transformação cultural, tecnológica e institucional; e, ainda, a capacidade para inovar, já que a inovação torna-se a principal arma competitiva." *Ibidem*.
[592] EUGÉNIO – ***Op cit.*** p. 61.

os princípios fundamentais da União, as disposições da CNU e as obrigações decorrentes da Resolução 1373 (2001) do CS das NU"[593].

Passados alguns anos, o CS das NU aprovou a Resolução n.º 2178, de 2014, a qual veio reafirmar que "o terrorismo em todas as formas e manifestações constitui uma das ameaças mais graves à paz e à segurança internacionais e que quaisquer atos de terrorismo são criminais e injustificáveis, independentemente de suas motivações, quando e por quem cometerem, e permanecendo determinado a contribuir ainda mais para melhorar a eficácia do esforço geral para combater esse flagelo em nível global". De igual modo, regista que "a ameaça terrorista se tornou mais difusa, com um aumento, em várias regiões do mundo, de atos terroristas, incluindo os motivados por intolerância ou extremismo, e expressando sua determinação em combater essa ameaça". Para concluir, a mesma regista "a necessidade de abordar as condições favoráveis à propagação do terrorismo e afirmando a determinação dos EM de continuarem a fazer tudo o que podem para resolver conflitos e negar aos grupos terroristas a capacidade de criar raízes e estabelecer refúgios seguros para enfrentar melhor a crescente ameaça representada pelo terrorismo", bem como reconhecendo que "a cooperação internacional e quaisquer medidas tomadas pelos EM para prevenir e combater o terrorismo devem estar em total conformidade com a CNU".

Por outro lado, não esqueçamos que os *media* potenciam os efeitos do terrorismo. Assim, recordando a Antiga Grécia, assinale-se que já "os sofistas procuravam descobrir meios de comunicação de persuasão na sociedade; hoje, os *media* e, em especial, a televisão, desempenham um papel primordial de influência. São protagonistas com capacidade de intervir, influenciar, desmascarar ou enaltecer outros intervenientes das Relações Internacionais"[594].

Face ao supracitado, poderemos asseverar que existem "cinco alterações fundamentais que diferenciam aquilo que era o terrorismo antes e depois do 11 de setembro: a cultura teocrática, que alavanca a predisposição para "morrer matando"; a estrutura organiza-

[593] Considera-se que a ameaça terrorista afeta a todos os EM da UE, pelo que um ato terrorista contra um país atinge a comunidade internacional no seu conjunto, não devendo haver fraquezas nem compromissos de qualquer espécie ao lidar com terroristas, uma vez que nenhum país do mundo se pode considerar imune, pelo que se entende que só a solidariedade e a ação colectiva poderão derrotar o terrorismo. CONSELHO EUROPEU – **Declaração sobre a luta contra o Terrorismo.** Bruxelas, 2004. p. 1.

[594] "Para além de utilizarem os *media*, os terroristas sabem como ampliar o valor-notícia, e fazem-no através da violência em grande escala. Michael Ignatieff afirma que os rebeldes *tchetchenos* foram pioneiros a filmar e a instalar a sensação de medo: "os terroristas foram rápidos a entender que a câmara tem o poder de emoldurar uma única atrocidade e transformá-la numa imagem que arrepia a espinha de todo um planeta. Este facto dá-lhes uma nova arma vital". Dois exemplos são o caso do teatro de Dubrovka (2002) e da escola de Beslan (2004)." LEMOS, Elsa – **Media e a gestão da percepção nas novas conflitualidades.** Lisboa: Academia Militar, 2012. Dissertação de Mestrado. p. 46-47.

cional fluida, de rede, que favorece a ligação com outras organizações e movimentos terroristas e que dificulta o seu aniquilamento; a imprevisibilidade; a perda da caraterística seletiva do alvo, que elege a população civil como alvo de excelência; e o facto de deixar de ser visto como um fenómeno de segurança interna para passar a ser encarado como um fenómeno internacional"[595].

Por outro lado, a evolução do terrorismo tem-no tornado num fenómeno com uma "organização específica, maleável, multicelular, servindo-se e servindo o crime organizado em grande escala, utilizando todos os recursos que a moderna tecnologia coloca à sua disposição"[596].

De igual modo, os "incidentes de terrorismo convencional já foram relacionados com o cibercrime e as vulnerabilidades nos sistemas de informação podem tornar um governo civil e os sistemas de infraestruturas críticas extremamente atraentes como alvos de um ataque cibernético"[597].

Para concluir este breve estudo sobre o terrorismo, acrescente-se que, no caso Nicarágua, o Tribunal de Haia considerou que "a mera assistência económica estadual a grupos rebeldes, apesar de indiscutivelmente constituir uma ingerência nos assuntos internos de outro Estado, não viola a proibição do uso da força", não obstante esta posição não ser pacífica[598].

2.2.2. O Ciberterrorismo

O ciberterrorismo pode ser concebido como a convergência entre o ciberespaço e o terrorismo, considerando os "ataques ilegais e as ameaças de ataques contra computadores, redes e informação aí armazenada quando estes forem realizados com o objetivo de intimidar ou coagir um governo ou o seu povo na persecução de objetivos sociais ou políticos"[599]. Em complemento, refira-se que "para ser caraterizado como um ato de ciberterro-

---

[595] VARINO – ***Op cit.*** p. 6.

[596] De acordo com o Professor Marques Guedes, o "aumento da pressão por parte dos Estados impeliu as organizações terroristas a adotarem uma organização em rede, como forma de garantir a sua segurança e aumentar a sua resiliência, pois verifica-se uma superioridade, quando em confronto, das redes policentradas sobre as estruturas hierárquicas." VARINO – ***Op cit.*** p. 8.

[597] MENEZES – ***Op cit.*** p. 25.

[598] "Resta saber se este entendimento não está hoje ultrapassado, pelo menos no que diz respeito à assistência económica prestada a grupos terroristas transnacionais. Parece ser esta a conclusão a retirar das resoluções do CS, adotadas ao abrigo do Capítulo VII logo após os ataques de 11 de setembro de 2001 em Nova Iorque, as quais reconhecem um direito de legítima defesa dos Estados perante ataques terroristas (Resolução 1368, de 12 de setembro de 2001) e impõe aos Estados a obrigação "de prevenir e suprimir o financiamento de atos terroristas" (Resolução 1373, de 28 de setembro de 2001)." COUTINHO – ***Op cit.*** p. 90.

[599] VIEGAS, Nunes – **Unidade Curricular de Guerra de Informação.** Mestrado em Guerra de Informação da Academia Militar – Ano letivo 2015/16. Slide 36.

rismo, um ataque deverá resultar em violência contra pessoas ou propriedade, ou em danos suficientemente elevados que gere medo"[600].

Deste modo, um ciberataque só deverá ser considerado um ato de ciberterrorismo se possuir objetivos políticos e originar um efeito direto, dramático e destrutivo.

Neste particular, surge o conceito de guerra cibernética, a qual pode ser definida como o "conjunto de ações ofensivas, defensivas ou exploratórias, realizadas no espaço cibernético, que buscam negar seu uso pelo inimigo, e garantir o uso da segurança, confiança, integridade, rapidez, sigilo das informações e tirar proveito próprio tanto na área militar quanto na área civil"[601].

Já o ataque cibernético pode ser entendido pela pluralidade dos "especialistas, não como uma arma contundente (como o é qualquer arma nuclear) mas como um complemento significativo nas guerras interestaduais[602]. Quanto aos grupos terroristas, lançam mão das ferramentas cibernéticas para destruir, embora o terrorismo cibernético estreitamente definido como o uso de ferramentas virtuais seja, até agora, raro"[603].Efetivamente, "os ataques cibernéticos parecem muito menos úteis que os ataques físicos: eles não enchem as vítimas potenciais de terror, não são fotogénicos e não são percebidos pela maioria das pessoas como eventos altamente emocionais"[604]. Deste modo, existem teorias que defendem que "as vulnerabilidades dos sistemas financeiros e elétricos são um alvo privilegiado para um qualquer grupo que deseje destruir; a isto há que adir a certeza de que tais grupos desenvolverão as potencialidades, de modo a tornarem-se uma ameaça maior do que os próprios Estados"[605]. Nas palavras de Mike McConnell, "quando os grupos terroristas tiverem a sofisticação, eles usar-la-ão"[606]. Com efeito, num passado recente, os explosivos têm sido "a ferramenta que melhor serve os objetivos dos terroristas, uma vez que o barulho e a

---

[600] *Ibidem*.
[601] "Os ataques cibernéticos podem ser classificados em três tipos diferentes: sociais, sofisticados e discretos. Os ataques cibernéticos sociais são aqueles que atacam as pessoas específicas utilizando a engenharia social e *malware* avançado; os ataques cibernéticos sofisticados exploram as vulnerabilidades nos sistemas de informação usando controlos de portas clandestinas, roubando e usando credenciais válidas; e os ataques cibernéticos discretos são executados numa série de movimentos discretos não detetáveis à segurança comum ou escondidos em milhares de registos de eventos recolhidos todos os dias." MENEZES – ***Op cit.*** p. 25.
[602] No que se reporta aos ataques cibernéticos que perturbam os sistemas ou negam o serviço também são perpetrados por agentes não-estatais, sendo os fins ideológicos ou criminais, sem que esses grupos tenham, no entanto, as mesmas capacidades que os grandes governos. Fáceis de levar à prática, são os ataques de baixo custo, como a negação de serviço contra destinos de baixo valor, como os *sites*.
[603] PARAÍSO, Ariana – Da sociedade em rede e do novo espectro de ameaças: o ciberespaço In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 54 Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2017. p. 15.
[604] *Ibidem*.
[605] *Ibidem*.
[606] NYE, Joseph – **Cyber Power. Technical Report.** Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010. p. 12.

comoção que provocam nas populações são mais consonantes com o seu *modus operandi*. Porém, tal não invalida que recorram à internet para promover o terrorismo: permite-lhes operar descentralizadamente, criar uma imagem identitária, recrutar simpatizantes para a sua causa, levantar fundos, prover manuais de treino e gerir operações, entre outras"[607].

Por outro lado, se o "hacktivismo é considerado como um problema menor, há, no entanto, que atender a quatro grandes ameaças cibernéticas à segurança nacional, correspondendo a cada uma tempos e soluções diferentes: espionagem económica, crime, guerra cibernética e terrorismo cibernético"[608].

A ciberguerra, "em sentido lato, designa algum tipo de «ataque» ou «represália», intrusão ilícita numa rede e/ou computador ou uma situação de espionagem[609] recorrendo, em qualquer dos casos a meios informáticos. As situações apontadas, podem ser ou não, associadas a conflitos de caráter político e/ou militar, no mundo real, isto é, ocorrer em paralelo com uma conflitualidade «física» ou de forma totalmente autónoma"[610].

O termo ciberguerra é igualmente utilizado para se referir a "uma guerra conduzida substancialmente no ciberespaço ou no domínio virtual"[611]; com efeito, aqueles que partilham de tal conceção "têm frequentemente em mente que as ciberguerras tendem a ser muito similares às guerras convencionais"[612], pelo que idênticas doutrinas de retaliação ou dissuasão poderão ser aplicadas.

Com efeito, no "ciberespaço, enquanto extensão virtual do mundo (físico e real), cumpre ao Estado o estabelecimento de normas e condutas a seguir, atribuindo responsabilidades e competências, na senda dos fundamentos que presidem à segurança e à defesa desse mesmo Estado"[613]. Tal, assenta na "crescente evolução das ciberameaças, quer na esfera nacional quer internacional, e que, naturalmente, afeta transversalmente toda a sociedade, prescrevendo a cibersegurança e a ciberdefesa do Estado como requisitos obrigatórios"[614]. Neste sentido, a dissuasão interestadual, a par das capacidades ofensivas e

---

[607] Exemplo deste uso terrorista da internet e das ferramentas cibernéticas disponíveis, a *Al Qaeda* suplantou-se, e da organização hierárquica constituída, com células geograficamente organizadas passou a ser para uma rede global à qual os voluntários locais se podem associar. PARAÍSO – ***Op cit.*** p. 15.
[608] NYE – ***Op cit.*** 2010. p. 16.
[609] Cfr. FERNANDES, José – A ciberguerra como nova dimensão dos conflitos do século XXI. In **Relações Internacionais.** Nº 33. 2012. (março) ISSN 1645-9199. p. 53.
[610] Cfr. BRANDES, Sean – **The Newest Warfighting Domain: Cyberspace.** [Em Linha]. 2013. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.synesisjournal.com/vol4_g/Brandes_2013_G90-95.pdf. p. 93. e PARAÍSO – ***Op cit.*** p. 16.
[611] FERNANDES – ***Op cit.*** p. 59.
[612] *Ibidem*.
[613] SANTOS, Lino et al. – ***Op cit.*** 2012. p. 168 a 174.
[614] Cfr. ARQUILLA, John; RONFELDT, David – **A New Epoch – and Spectrum – of Conflict**. 2000. p. 6.

uma maior resiliência, afiguram-se como instrumentos de gestão da guerra cibernética. Em complemento, e no "caso da guerra "física", ao combate seriam aplicados critérios de discriminação e proporcionalidade a partir de leis existentes de conflitos armados, embora haja problemas na distinção de alvos civis de militares, e de ter a perceção sobre a extensão dos danos colaterais"[615].

Por outro lado, e recorrendo ao evento *Web Summit* 2018[616], Jared Cohen[617] explicou porque "todas as guerras vão começar como ciberguerras"[618], acrescentando que a Terceira Guerra Mundial pode ter início no mundo digital. O mesmo abordou aquela que considera ser a "grande interrogação tecnológica e geopolítica do momento: como podemos prevenir uma ciberguerra?" A resposta pautou-se por pretender alertar para a realidade atual, bem como tranquilizar a plateia devido ao espírito inovador dos empreendedores que o estavam a ouvir. A sua intervenção referiu que "dentro de três anos, haverá mais dispositivos inteligentes em circulação do que seres humanos no planeta", considerando a omnipresença e fluidez da tecnologia atual[619]. O mesmo acrescenta ainda que, "o que existe hoje é um sistema internacional que tem uma frente física e uma frente digital, e todos os desafios do mundo físico que conhecemos há décadas e séculos estão a derramar para o *online*", motivo pelo qual sustenta que "todas as guerras vão começar como ciberguerras". De igual modo, complementou com o facto de ser "a economia, a política e o poder militar a determinar quais são os Estados mais poderosos"[620].

Apesar de, formalmente, não haver registo de uma declaração de um Estado de "ciberguerra a outro, todos os dias militares e espiões lançam campanhas contra servidores

---

[615] PARAÍSO – ***Op cit.*** p. 18.

[616] A *Web Summit* decorreu em 2018 em Lisboa. Esta cimeira tecnológica, de inovação e de empreendedorismo nasceu em 2010 na Irlanda e mudou-se em 2016 para Lisboa por três anos, com possibilidade de mais dois de permanência na capital portuguesa.

[617] O presidente executivo da Google Jigsaw, uma aceleradora que investe e estuda os impactos da geopolítica, frisou que estamos prestes a entrar numa era mais complexa do que a do mundo bipolarizado da Guerra Fria, do mundo unipolar do pós-Guerra Fria e do mundo multipolar pós-11 de setembro.

[618] [Consult. 27 Mar. 2019]. Disponível em WWW:<URL: http://24.sapo.pt/tecnologia/art.ºs/web-summit-todas-as-guerras-vao-comecar-como-ciberguerras.

[619]"No *Center Stage* da *Web Summit*, Jared Cohen recordou que a internet é uma moeda de duas faces, onde não figuram apenas as "histórias extraordinárias sobre como a tecnologia mudou para sempre a vida de milhões de pessoas". Ainda que estas existam, diluem-se cada vez mais entre as narrativas sobre como a internet criou mecanismos para magoar, destruir e aniquilar. Se, por um lado, é capaz de dar "uma segunda oportunidade de viver" a uma mulher afegã violentada por um grupo terrorista talibã; por outro é montra e veículo de recrutamento para grupos como o autoproclamado Estado Islâmico. "E não importa se os vídeos são pouco editados, se parecem amadores ou exagerados. Os destinatários não querem saber desses detalhes. O importante é a mensagem". E muitas vezes a mensagem é nada mais, nada menos, que "propaganda"."

[620] Estes atributos permanecem inalterados. "Só que, doravante, os estados mais poderosos serão aqueles capazes de projetar influência nessas áreas, mas em ambos os domínios: o físico e o virtual".

e computadores no estrangeiro"[621], pelo que a ciberguerra existe e poderá estar em vias de se desenvolver.

Os ciberataques têm um enorme potencial disruptivo, motivo pelo qual as principais potências cibernéticas têm travado os seus ímpetos, considerando que é "o receio de ser alvo de uma retaliação de grandes proporções que tem prevalecido sobre o lançamento de ataques contra infraestruturas críticas"[622], pelo que "os ataques danosos, típicos do ciberterrorismo, tendem a ser reservados apenas para as situações em que não há alternativa"[623].

Por outro lado, registe-se que não é expectável que passemos a ter cenários de guerra sem sangue. Todavia, o que passará a existir é um cenário de guerra em que as primeiras ações poderão decorrer com o recurso a "um conjunto de ciberataques usando drones, robôs ou a internet com o objetivo de um país (…) e só depois, eventualmente, avançar para a guerra convencional, que já poderá tirar partido dessa neutralização para ocupar um território com um número de perdas de vidas mínimo"[624], prevê António Nunes, presidente do Observatório de Segurança, Criminalidade Organizada e Terrorismo (OSCOT).

Todavia, os atos de ciberterrorismo serão, na sua maioria, menos comuns do que os de ciberespionagem, uma vez que o impacto do primeiro está dependente do fenómeno mediático, ao contrário do segundo. Com efeito, "ao contrário da ciberespionagem, o impacto do ciberterrorismo depende em grande parte da divulgação alcançada"[625].

Já no final de 2003 foi aprovada a designada Estratégia de Segurança Europeia (ESE), no sentido de superar a incapacidade da UE de se colocar de forma unida e influente no contexto da Guerra do Iraque. Este é considerado um documento de referência que tem suportado as manobras europeias que tenham relação com questões políticas e de segurança. A ESE identificou as principais ameaças para a segurança europeia[626], mas também as principais formas de combatê-las. Em 2008, "os EM sancionaram o Relatório para a Implementação da ESE, que veio a reforçar o primeiro documento, especialmente ao adi-

[621] "Em 2010, a Secretária de Estado Hillary Clinton protagonizou a primeira acusação oficial de ciberataques de uma Nação contra outra. Na origem da acusação, esteve uma campanha de Ciberataques a várias instituições dos EUA que ficou conhecida com Aurora." SÉNECA, HUGO – A guerra não acabou. Nem vai acabar. In **Exame Informática.** Fevereiro de 2017. p. 59.
[622] A própria interdependência que carateriza as sociedades em rede tem inibido ações mais violentas, devido ao impacto económico que o caos registado de súbito num país pode gerar na comunidade internacional. *Ibidem*.
[623] SÉNECA – ***Op cit.*** p. 63.
[624] SÉNECA – ***Op cit.*** p. 64.
[625] *Ibidem*.
[626] Por exemplo, terrorismo transnacional, armas de destruição em massa, estados-falidos, conflitos regionais e o crime organizado.

cionar à lista de ameaças algumas grandes preocupações, tais como, terrorismo cibernético, pirataria, mudanças climáticas, e segurança energética"[627].

O Tratado de Lisboa veio definir a utilização no exterior da capacidade operacional da UE no âmbito das missões previstas pela PCSD, a qual contempla missões conjuntas em matéria de desarmamento, missões humanitárias e de evacuação, missões de aconselhamento e assistência em matéria militar, missões de prevenção de conflitos e de manutenção da paz, bem como missões de forças de combate para a gestão de crises[628], nos termos do art.º 42.º, n.º 1, do TUE, e de acordo com os princípios da CNU.

Em dezembro de 2016, o Conselho Europeu aprovou o plano de execução em matéria de segurança e defesa, o qual define o caminho a seguir para desenvolver a política de segurança e defesa da UE[629].

Com efeito, a agenda da UE tem uma relevância "externa", já que procura dar resposta a 3 ameaças: terrorismo, criminalidade organizada e cibercriminalidade"[630].

Neste particular temos observado que o cibercrime é utilizado numa estrutura organizada de financiamento ao terrorismo.

Assim, constatamos que o ciberespaço foi "na realidade uma oportunidade única de expansão e solidificação de um mercado criminoso emergente"[631].

Deste modo, as redes de crime organizado ao passarem a atuar no ciberespaço deram origem a "um novo tipo de crime que se verificou uma fonte muito rentável, que possui poucos riscos e que, finalmente, é anónima, [pelo que é] importante definir que o cibercrime é diferente do ciberterrorismo, pois o primeiro serve como estrutura de movimentação e angariação de fundos, a par que o segundo extravasa esse sentido apenas mantendo em comum o meio de ação e o aproveitamento das regalias do mesmo"[632].

---

[627] FERREIRA-PEREIRA, Laura – **A Política Europeia de Segurança e Defesa após o Tratado de Lisboa: estado da arte e perspectivas futuras.** KA Cadernos, 2013. p. 65-71.

[628] Incluindo as missões de restabelecimento da paz e as operações de estabilização de conflitos.

[629] [Consult. 27 Mar. 2019]. Disponível em WWW:<URL: https://www.consilium.europa.eu/pt/policies/defence-security/.

[630] MASSENO, Manuel - Garantir a Cibersegurança e a Ciberdefesa à custa dos Cidadãos? In **IX Simpósio sobre Segurança Informática e Cibercrime.** SimSIC: Beja, 2018. Slide 10.

[631] MILITÃO – ***Op cit.*** p. 42.

[632] "Para grupos terroristas e para redes de crime organizado o simples roubo de dados de acesso a contas bancárias, ou o acesso a linhas de crédito significam o acesso a fundos de financiamento para as suas ações. Estes grupos roubam identidades e posteriormente utilizam-nas para obter créditos em diversos bancos. Um dos mais notáveis indivíduos a conseguir uma proeza deste género, financiar atos terroristas com recurso a financiamento pela prática do cibercrime, foi um dos bombistas da *Al-Qaeda*, conhecido como o Bombista de Bali."Por outro lado, a sua "metodologia de ação pode ser individual ou em pequenos grupos nos quais cada membro exerce uma função na construção de um *malware*, podendo não estarem aparentemente relacionados uns com os outros". MILITÃO – ***Op cit.*** p. 43 e 45.

Por outro lado, o cibercrime "atingiu proporções dramáticas, e uma grande fatia desta razão assenta na necessidade que grandes grupos terroristas ou redes de crime organizados têm em arranjar fundos de fontes com as quais dificilmente podem ser identificados"[633].

Desta forma, surge então a necessidade de uma cooperação internacional em matéria de cibercrime. As "autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais"[634], previstas na Lei n.º 58/2019, de 08 de agosto.

De igual modo, a Lei do Cibercrime preconiza no seu art.º 20.º relativo ao âmbito da cooperação internacional, que com "o intuito de manter a integridade nacional, cada Estado almeja uma construção própria nacional, de um dado tipo de estrutura que consiga garantir um mínimo de segurança neste novo meio, a par com os outros que já possuía nomeadamente, as FA e as forças de segurança". Para a sua prossecução, "os Estados na sua maioria, dotaram as forças já existentes, de segurança e militares, de novas capacidades, cujo objetivo seria não só atuar em caso de ataque, mas também de prevenção e mitigação do crime por este meio"[635].

Por outro lado, o "crescimento exponencial de perigos associados ao ciberespaço trouxe novos desafios às entidades que procuram regular os crimes efetuados através deste meio"[636], tal como é o caso das fraudes *online*, as quais "provocaram uma evolução nas relações de articulação entre diferentes organismos supra estatais que procuram regular e fiscalizar as ações criminosas no ciberespaço"[637].

Com efeito, o "ciberespaço constitui um desafio à Ordem Vestefaliana, pois coloca em causa a territorialidade, a soberania e a autonomia de um Estado, verificando-se necessário alterar esses pressupostos"[638]. Deste modo, a existência de "uma ciberdefesa e de uma cibersegurança eficazes são o princípio de criação de fronteiras no ciberespaço, pois estas revelam que um só responsável pela sua segurança seria perfeitamente incapaz de arcar com as necessidades requeridas"[639].

---

[633] MILITÃO – ***Op cit.*** p. 45.
[634] MILITÃO – ***Op cit.*** p. 52.
[635] MILITÃO – ***Op cit.*** p. 62.
[636] MILITÃO – ***Op cit.*** p. 65.
[637] *Ibidem*.
[638] MILITÃO – ***Op cit.*** p. 77.
[639] *Ibidem*.

Neste sentido, constatamos que o "grande aumento da cibercriminalidade deve-se portanto às potencialidades do ciberespaço enquanto rede intrincada de acessos que promovem uma interligação rápida e facilitada às fontes que provem o que os cibercriminosos procuram". Para mitigar estes factos, verifica-se uma elevada "necessidade de criar estruturas nacionais e internacionais que interligadas funcionem como uma rede exclusiva à prevenção do cibercrime, muito como as equipas especializadas no combate à cibercriminalidade fora do ciberespaço"[640].

Outro aspeto importante, prende-se com a eventual alteração de poderes a nível mundial, devido à "utilização do ciberespaço enquanto meio de propaganda e de recurso aos *media*, mas também devido à visibilidade internacional de vanguarda. O ciberespaço é hoje um meio definitivo na denominação de potência internacional, no mesmo patamar que os outros meios, pois proporciona aos Estados que dele se aproveitam uma posição de controlo e liderança cujo objetivo último é que os seus ganhos de vitória sejam muito superiores às perdas em caso de derrota"[641].

Como tal, o ciberterrorismo é geralmente definido como "todos os ataques altamente prejudiciais a computadores, projetados por indivíduos que procuram gerar o terror e o medo para atingir objetivos políticos ou sociais"[642].

Este tipo de terrorismo surge da convergência entre o ciberespaço e o terrorismo. Isto é, o "terrorismo enquanto atividade de cariz político ou social, com vítimas indiscriminadas, que procura instalar o terror e o pânico nas sociedades, aproveita-se das caraterísticas da internet para atingir tais fins, agora a uma escala global"[643].

Deste modo, constate-se que "um ataque para ser qualificado como ciberterrorista deve resultar em violência contra pessoas ou bens ou, pelo menos, causar dano suficiente para gerar medo. Ou seja, o ciberterrorismo é a utilização do ciberespaço para alcançar os

---

[640] "Teoricamente já existem equipas que visam a prossecução não só deste objetivo mas também da prevenção de práticas ciberterroristas, da monitorização e prática de ciberespionagem e, finalmente, equipas prontas para agir em caso de ciberguerra." *Ibidem*.

[641] MILITÃO – ***Op cit.*** p. 77.

[642] WARREN, M. – **Terrorism and the Internet. Cyber Warfare and Cyber Terrorism.** Information Science Reference, 2008. p. 129.

[643] O terrorismo tradicional aproveita-se assim das novas formas de comunicação para fazer cumprir os seus objetivos, tendo evoluído em termos de operacionalidade, representando agora uma nova e grande ameaça aos Estados, cujo combate se afigura como difícil e desafiante. Sumariamente, o ciberterrorismo será definido como "o uso das TIC para a realização de ameaças ou [para] a organização (incluindo a troca de informação, angariação de seguidores e financiamento) e execução de ataques com grande impacto nas redes e sistemas informáticos e nas infraestruturas críticas, motivadas por ideologias políticas ou religiosas, fomentando o medo e o terror, com intuito de despoletar determinadas ações políticas". BARBOSA – ***Op cit.*** p. 10.

mesmos objetivos ou objetivos semelhantes do terrorismo tradicional"[644].Assim, os "ataques que apenas provocam disrupção de serviços não essenciais ou são principalmente perdas financeiras irrelevantes"[645] não são considerados como ciberterrorismo.

No que respeita à ciberespionagem, a mesma é "levada a cabo por Estados que procuram adquirir conhecimento e recolher informações que lhes possam conceder uma vantagem estratégica sobre terceiros"[646], sendo uma variante da espionagem tradicional.

A ciberespionagem consiste "na obtenção de informações, que podem pertencer a empresas ou Estados, para benefício próprio destes ou para obter um benefício monetário posterior com a sua venda a outras entidades"[647].

Voltando ao ciberterrorismo, a UE define-o como uma forma de atividade terrorista que visa "destruir ou deteriorar sistemas informáticos como as bases de dados civis ou militares, ou sistemas de telecomunicações, com o fim de destabilizar o Estado ou exercer pressão sobre os poderes públicos"[648].

Deste modo, assinale-se que "não é apenas através de técnicas de *hacking* que um terrorista pode efetuar um ataque a uma infraestrutura, [pelo que] sem haver uma intrusão, o terrorista pode como complemento a um ataque convencional utilizar técnicas de disrupção de efeito imprevisto através de *worms*"[649].

Outra dificuldade reside no facto de que qualquer internauta poderá utilizar mensagens com uma cifra forte, estando esta disponível a nível gratuito na internet[650].

---

[644] "Ataques sobre as IC que afetem gravemente a vida de pessoas, que causem explosões ou perdas económicas graves são exemplos de ataques ciberterroristas". VARINO – ***Op cit.*** p. 10.

[645] SILVA, Tiago – **A ameaça terrorista em Portugal.** Lisboa: Universidade Nova de Lisboa, Faculdade de Ciências Sociais e Humanas, 2015. Tese de Doutoramento. p. 79.

[646] "Esta ameaça carateriza-se pela exploração das vulnerabilidades encontradas nos *websites* (geralmente governamentais e de empresas), acedendo a informação sensível, muitas vezes com o intuito de roubar informação sobre projetos em desenvolvimento ou segredos de negócio. As motivações por trás da ciberespionagem consistem na vantagem competitiva de Estados sobre Estados ou de empresas sobre outras empresas que desenvolvam projetos na mesma área, ou ainda os benefícios financeiros da venda da informação roubada." BARBOSA– ***Op cit.*** p. 11.

[647] *Ibidem*.

[648] SILVA – ***Op cit.*** p. 79.

[649] Outros ataques informáticos podem ser tomados pelo terrorismo (alteração de páginas *web*, envio massivo de *spam* (correio eletrónico não solicitado), roubo de números de cartão de crédito e fraude informática), uma vez que o funcionamento da internet dificulta a "deteção do terrorista informático visto que a informação circula de forma independente através de circuitos e equipamentos de comutação por *routers*. Além disso, o terrorista informático pode apagar os indícios que o poderiam incriminar, através de técnicas de *spoofing* (alteração de cabeçalhos em mensagem de correio eletrónico, a alteração de endereço IP da origem da comunicação ou a alteração de endereço MAC do computador ou terminal móvel usado) ou efetuar os ataques num cibercafé, [pelo que] os ataques podem acontecer em países onde a criminalização deste tipo de ações não existe e os meios de investigação criminal são deficientes para este tipo de ações". SILVA – ***Op cit.*** p. 82.

[650] Na casa do terrorista Ramzi Yousef foram encontradas mensagens cifradas que levaram um ano a serem descodificadas pelo FBI sobre a destruição de 11 linhas aéreas norte americanas.

Face ao exposto, é importante percebermos que o "terrorismo pode estar num computador ligado a uma rede e pode criar uma confusão à escala mundial"[651]. Assim, já antes dos acontecimentos do 11 de setembro, o presidente Bush tinha aludido ao perigo iminente de um ataque aos EUA por ciberterroristas, ao avisar durante a sua campanha presidencial que as FSS americanas estavam "prontas a enfrentar um conjunto de novas ameaças e desafios – a disseminação de armas de destruição massiva, o aumento de ciberterrorismo, a proliferação de mísseis (tecnológicos)"[652].

Por outro lado, recordemos que os sistemas de informação desempenham um papel fundamental na nossa sociedade. Porém, por vezes, os mesmos acabam por potenciar alguns focos de instabilidade e originar conflitos que podem colocar em causa os objetivos últimos dos Estados: a segurança, a prosperidade e o bem-estar social do seu povo[653]. Neste contexto, recordemos os exemplos dos "ataques de 2007 na Estónia, de 2008 na Geórgia, no caso *Wikileaks* ou nos ataques do grupo Lulzsec Portugal, efetuados em 2011"[654].

Assim, a crescente importância da internet e destes sistemas despoletaram o surgimento dos "termos cibercrime[655], ciberguerra, ciberataque, cibersegurança e ciberterrorismo, levando os países e organizações a preocuparem-se e prepararem-se para esta realidade, criando estruturas e procedimentos de defesa e de combate para lhes fazer face"[656].

Deste modo, o ciberespaço tem-se constituído como "um autêntico campo de batalha digital, onde indivíduos, organizações e até mesmo Estados têm executado ações ofensivas e defensivas, de forma a atingirem os seus objetivos"[657].

---

[651] SILVA – ***Op cit.*** p. 83.

[652] Magnus Ranstorp, diz que a internet e as telecomunicações, inclusive por satélite, são usadas como "uma infinita estrada de comunicação pelos terroristas" e que embora isto permita a monitorização dos serviços de espionagem, as células dominam o meio utilizando ficheiros encriptados, cartões de telemóvel pré-comprados, mensagens de *spam* sinalizadas, e *chats* comuns. Uma das táticas de cobertura utilizadas é a abertura de contas no Yahoo e no Hotmail, com nomes e códigos, permitindo a escrita, na caixa de mensagens, que nunca são enviadas, mas se tornam acessíveis para os membros da célula que conhecem o código de acesso. Para Ranstorp "é claro que a *Al-Qaeda* investiu fortemente no conhecimento e no uso das infinitas vias criadas pelo ciberespaço". SILVA – ***Op cit.*** p. 83-84.

[653] "Fruto da enorme evolução tecnológica e da crescente automatização de todas as áreas de atividade das sociedades atuais, o ciberespaço surge como um novo espaço virtual de interação económica, social e cultural. As sociedades industriais, especialmente as que vivem num sistema de mercado livre e aberto, apresentam uma grande dependência relativamente às redes e sistemas de informação que estão na base do seu processo de geração de riqueza e de bem-estar social." VARINO – ***Op cit.*** p. 10.

[654] VARINO – ***Op cit.*** p. 9.

[655] "O cibercrime é um ato praticado contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a sua utilização fraudulenta. Incluem acesso e interceção ilegítima, interferência em dados e sistemas, uso abusivo de dispositivos, falsidade e burla informática, infrações relacionadas com pornografia infantil e violação do direito de autor." Segundo a Interpol, é uma das áreas de maior crescimento da criminalidade. VARINO – ***Op cit.*** p. 10-11.

[656] VARINO – ***Op cit.*** p. 10.

[657] Neste novo campo de batalha o ciberterrorismo prolifera e, "ao contrário das guerras convencionais que envolvem homens fortemente armados, uma grande estrutura de defesa e segurança, esta é uma guerra

2.2.3. Os Ataques Maliciosos

Neste subcapítulo iremos abordar alguns dos ataques maliciosos mais conhecidos, a saber: *malware*, *DoS*, *DDoS*, *ransomware*, vírus, entre outros.

Todavia, antes de mais importa aqui recordar que os ciberataques se dividem em três formas básicas: "ataques sobre a confidencialidade dos dados, que abrange qualquer aquisição não autorizada de informações; ataques sobre a integridade da informação, que inclui a sabotagem de dados com objetivos criminosos, políticos ou militares; e os ataques sobre a disponibilidade de computadores ou recursos de informação. Esta terceira forma tem como objetivo evitar que os utilizadores autorizados tenham acesso aos sistemas ou aos dados de que necessitam para executar determinadas tarefas[658]„[659].

Em complemento, atente-se que existem uma multiplicidade de métodos, os quais podem incluir: "ataques para invadir ou para obter o controlo sobre a rede; vírus de computador e *worms* que modificam e destroem informações ou prejudicam o funcionamento dos sistemas dos computadores; bombas lógicas que se instalam nos sistemas operativos dos computadores e permanecem em hibernação até serem acionadas, causando a destruição dos sistemas hospedeiros; e, ainda, *trojans* que permitem a execução de certas ações sem o conhecimento do proprietário do sistema comprometido"[660].

O primeiro ataque malicioso que iremos analisar é o *malware*, apesar de não se tratar de um tipo único de ataque, uma vez que os *softwares* maliciosos podem assumir diversas formas. Deste modo, o "*malware* pode incluir formas tão diferentes de ataque quanto vírus, *worms*[661], *trojans*, *spyware*, *adware* e o próprio *ramsomware*. Este tipo de ficheiros permi-

---

moderna sem rosto, sem identidade e sem as fronteiras físicas do Estado. Algumas das principais caraterísticas dos ciberataques são que podem ser conduzidos remotamente, no anonimato, são baratos, não exigem o uso de explosivos ou suicidas e são de difícil prevenção e combate porque podem ser efetuados de qualquer parte do mundo." Por outro lado, "os terroristas, além de utilizarem o ciberespaço para atividades estritamente ciberterroristas, utilizam-no também para facilitar e complementar as formas tradicionais de terrorismo, como por exemplo os atentados, potenciando, de forma exponencial, os seus efeitos, incluindo os mediáticos. [Estes] usam a internet como meio de comando e controlo, comunicando e passando informações sobre possíveis alvos, utilizando mensagens de correio eletrónico cifradas, e também para fins propagandísticos, publicitando a sua causa com o objetivo de angariar fundos e recrutar seguidores. Utilizam não só os *websites* já disponíveis, como criam *websites* para as próprias organizações." VARINO – ***Op cit.*** p. 11-13.

[658] As ações que concretizam este objetivo são comummente referidas como negações de serviço (*DoS*) e abrangem o tráfego de rede ou ataques físicos a computadores, bases de dados e às redes que os ligam.

[659] VARINO – ***Op cit.*** p. 11.

[660] VARINO – ***Op cit.*** p. 11-12.

[661] "Os *worms*, em particular, tendem a assumir níveis crescentes de complexidade, sendo cada vez mais difíceis de detetar por antivírus, *antimalware* ou *firewalls*. Num mundo altamente competitivo, qualquer vulnerabilidade no sistema de informação de uma empresa pode destruir-lhe por completo o negócio, ou retirar-lhe a vantagem competitiva sobre um concorrente. Por essa razão, e pelo facto de praticamente todas

te roubar, danificar, modificar, destruir ou impedir o acesso aos dados, podendo comprometer o funcionamento de toda uma instituição, provocando enormes prejuízos"[662].

Em complemento, refira-se que diariamente se verifica o aparecimento de novo *malware*, isto é, "*software* que procura danificar computadores ou sistemas, com tendência para um aumento acentuado"[663].

Por outro lado, a designação de *hacking* refere-se à "utilização de uma ferramenta para um fim diferente daquele que foi originalmente desenvolvida, [uma vez que]os *hackers*, no domínio cibernético, são motivados por razões ideológicas, de desafio e reconhecimento na comunidade e cada vez mais por motivos financeiros. Quando a técnica de *hacking* procura atingir objetivos políticos, estamos na presença de *hacktivismo*"[664].

Outro tipo de ataque é o *DoS*, ou seja, um ataque de negação de serviço. Este tipo de ataque pretende o bloqueio do "acesso a sistemas críticos, como *sites* ou *email*, sobrecarregando-os com tráfego de internet, e podem causar destruição financeira e interromper as operações normais"[665].

Já os ataques distribuídos de negação de serviço(*DDoS*), a sua principal função não é a de "destruir os recursos do alvo, mas antes impedir o acesso aos mesmos, mediante uma sobrecarga do sistema, o que pode ser feito, essencialmente, de duas formas: consumo de recursos da máquina, tais como memória ou processamento (recorrendo a *worms*, por exemplo), ou a uma sobrecarga dos servidores como resultado de um simultâneo e elevadíssimo nível de acessos (por exemplo, recurso a *botnets*)"[666].

O *ramsomware* é um tipo de *malware*, o qual tem registado um aumento de tipos de ataque, "uma vez que a motivação por detrás do *ramsomware* é essencialmente económica, pertencendo ao domínio da extorsão ou da fraude. Com efeito, esta modalidade de *malware* impede o acesso aos dados por parte do utilizador, sendo o mesmo restabelecido após o pagamento de um resgate. Mas pode tratar-se de um crime mais complexo, quando o ata-

---

as instituições se encontrarem ligadas a um qualquer tipo de rede, e portanto vulneráveis, não é expectável que esse tipo de ataques venha a diminuir." RODRIGUES – ***Op cit.*** 2016. p. 15.

[662] *Ibidem*.

[663] ANTUNES – ***Op cit.*** p. 1.

[664] "Apesar da aparente clareza da definição, neste tipo de atividade nada é claro e facilmente se confunde o ciberativismo social e político com vandalismo ou ciberterrorismo. Como exemplos, observemos: na invasão do Iraque, alguns *sites* governamentais dos EUA foram modificados, num claro protesto contra a guerra e incitando à recreação; os apoiantes de Julian Assange (fundador do *Wikileaks*.) lançaram ataques contra instituições de crédito; os vários episódios ocorridos durante a Primavera Árabe, em que entidades governamentais e *hackers* apoiantes da democracia se digladiaram na internet. Grupos organizados, organizações internacionais ou países podem patrocinar o hacktivismo neutralizando ou danificando profundamente as infraestruturas críticas de um estado." *Ibidem*.

[665] SYMANTEC – **Relatório de Ameaças à Segurança de Sites.** 2015. p. 18.

[666] RODRIGUES – ***Op cit.*** 2016. p. 14.

cante não pretende, ou não é capaz, de restabelecer os dados roubados ou o acesso aos mesmos"[667], uma vez que "os criminosos usam *malware* para criptografar os dados dos discos rígidos das vítimas e exigem pagamento para desbloquear os arquivos"[668].

Neste contexto, não esqueçamos que o anonimato propiciado pela internet, tende a estimular os criminosos a "explorar essa janela de oportunidade proporcionada pela venda de produtos desenvolvidos por *black hat hackers*[669] ou informáticos altamente especializados que colocam as suas enormes capacidades ao serviço do crime organizado"[670].

O vírus é outro método de ataque genericamente conhecido como uma ameaça no ciberespaço[671]. A sua designação provém da comparação com o vírus biológico que precisa do ADN de uma célula para se replicar e exercer a sua ação nociva sobre o organismo. Assim, este vírus informático apropria-se "dos ficheiros executáveis de um sistema, para se disseminarem e infetá-lo. Alguns vírus são concebidos para se manifestarem somente em determinadas datas, podendo, para além dos computadores, exercer a sua ação em telemóveis, o que aumenta o seu potencial de ameaça no seio das organizações"[672].

Em relação aos *worms*, a sua principal função é explorar as vulnerabilidades no *software* dos computadores. "Ao contrário dos vírus, os worms não necessitam dos ficheiros do hospedeiro para se auto replicarem. Podem apagar ficheiros do computador infetado, enviar emails não desejados ou criar novas vulnerabilidades num sistema de informação em rede, podendo ser utilizados em *DDoS*"[673].

Quanto aos *trojans*, geralmente são benignos, sendo que podem igualmente executar "instruções hostis, de uma forma que escapa ao controlo do utilizador do computador. Normalmente introduzem-se a partir de mensagens de *email*, podendo criar vulnerabilidades no sistema, conduzir ao roubo de dados ou à alteração de configurações"[674].

Os *bots*, tal como os *worms*, são capazes de "propagar-se automaticamente, sendo capaz[es] de proporcionar o controlo remoto de um computador (ou vários, no caso das

---

[667] RODRIGUES – ***Op cit.*** 2016. p. 15.
[668] "A melhor e praticamente única defesa é manter um *backup* separado dos arquivos, de preferência *offline*, para futura restauração. Existem muitas variantes de *ransomware*, e nenhum sistema operacional garante imunidade." SYMANTEC – ***Op cit.*** p. 27.
[669] Também designados como *crackers*, tal como veremos nas próximas páginas.
[670] RODRIGUES – ***Op cit.*** 2016. p. 15.
[671] Apesar de estar a ser progressivamente substituído pelos *worms* nos rankings de ocorrência de ataques, nos vários países.
[672] RODRIGUES – ***Op cit.*** 2016. p. 16.
[673] Estes são "grandes consumidores de recursos, devido ao elevado número de cópias que costumam fazer de si próprios, podendo afetar de um modo decisivo o desempenho de uma máquina, ou mesmo de uma rede." *Ibidem*.
[674] RODRIGUES – ***Op cit.*** 2016. p. 17.

botnets), que passa a ser utilizado em ações hostis, sem o conhecimento do respetivo proprietário, sendo as mais comuns, as negações de serviço"[675].

No que respeita ao s*pyware*, este trata-se de um "programa que possibilita o envio de informações de um computador para terceiros, sem o conhecimento e autorização do respectivo proprietário"[676].

Após termos analisado alguns dos ataques maliciosos mais conhecidos, vamos agora observar os utilizadores de internet e quais os papeis que podem representar. Assim temos:

a) *Hackers (white-hats)*: são os utilizadores que conseguem superar até os limites das máquinas e dos programas, caraterizando-se por serem uns curiosos por natureza, pessoas que têm em aprender e se desenvolver um *hobby*, assim como ajudar os menos favorecidos. Os *hacker*s em geral partem do princípio de que todo sistema de segurança tem uma falha, e a função deles é encontrar essa "porta".[677]

b) *Crackers (black-hats)*: este vocábulo tem a sua origem no verbo em inglês "*to crack*", o que se traduz em "quebrar códigos de segurança". Estes utilizadores têm um "alto grau de conhecimento e nenhuma ética, [considerando que] os *cracker*s invadem sistemas e podem apenas deixar a sua "marca" ou destruí-los completamente".Regra geral, estes são *hacker*s que se querem vingar de algum operador, adolescentes que pretendem ser aceites em grupos de *cracker*s (ou *script-kiddies*) e que acabam por apagar tudo o que vêem, ou então são *experts* de programação que são pagos por empresas para fazerem espionagem industrial".[678]

c) *Phreakers*: os *phreaker*s são os maníacos por telefonia, os quais utilizam "programas e equipamentos que fazem com que possam utilizar telefones gratuitamente, [pelo que] se consideram uma categoria à parte, uma vez que podem ser *hacker*s, *cracker*s ou nenhum dos dois"[679].

---

[675] Os *bots* são "muito eficazes nas situações em que os atacantes pretendem camuflar a origem dos ataques, e no envio de *spam*". *Ibidem.*

[676] "As formas mais conhecidas de *spyware* são: a) *keylogger*: permite identificar as teclas utilizadas pelo utilizador do computador, tornando possível a obtenção indevida de códigos ou *passwords*; muito utilizado em ações hostis no âmbito do *homebanking* e do comércio electrónico. b) *screenlogger*: usado para determinar as teclas pressionadas pelos utilizadores de teclados virtuais; permite determinar a posição do cursor (e sua evolução) numa página específica, também ela visualizável. c) *adware*: inicialmente projetado para fins publicitários, pode assumir um carácter ilegítimo a partir do momento em que a navegação do utilizador é monitorizada sem o seu conhecimento, resultando muitas vezes no envio de publicidade indesejada ou em situações de violação de privacidade. d) *backdoor*: Programa que cria as condições para o retorno de um invasor a um computador comprometido." *Ibidem.*

[677] SILVA, Andréia; SOARES, Cínthia; ULYSSÉA, Isabelle – **Hackers e Crackers**. Brasília: Universidade Católica de Brasília, [s. d.]. Trabalho de Pós-Graduação. p. 3.

[678] *Ibidem*.

[679] *Ibidem.*

Por outro lado, a prática de *hacking* pode ser motivada por diversos motivos, a saber[680]: insatisfação de funcionários com a empresa em que trabalha(va)m[681]; fama[682]; manifesto[683]; ou para ganhar dinheiro[684].

A fim de mitigar os variados ataques maliciosos, as organizações têm de assegurar uma capacidade de resposta a estes ataques informáticos, através da segurança informática.

Para tal, as organizações "com redes informáticas, conjugam normas e procedimentos de segurança com sistemas de proteção periféricos como *firewalls*, *intrusion detection system*, antivírus, que no passado revelaram alguma eficácia, mas face à complexidade das ciberameaças, têm-se revelado insuficientes"[685]. Assim, o modelo de defesa em profundidade aplicado à segurança dos sistemas de informação afigura-se como uma boa solução, considerando que neste modelo são utilizadas várias camadas de proteção para os dados.[686]

Estes modelos para "sistemas de defesa modernos apoiam-se nos "sistemas de sistemas", [que] tirando partido do comportamento coletivo oferecem vantagens relativamente aos que atuam de forma individual. Estes sistemas podem ser regulados pelas mais variadas entidades e, uma vez que possuem capacidades C2[687], é necessário garantir que os seus utilizadores obtêm a consciência situacional necessária ao ciberespaço"[688].

Do ponto de vista organizacional, os *Computer Emergency Response Team* (CERT[689]) têm-se constituído como "a forma plausível de manter a continuidade de negócio das organizações e no limite dos Estados"[690].

---

[680] SILVA – ***Op cit.*** [s. d.]. p. 9.

[681] "Segundo especialistas, a maior parte das invasões acontece ou são planeadas de dentro das empresas atacadas. Esses ataques podem também ser fruto de concorrência entre empresas, que contratam *crackers* para praticar espionagem e provocar prejuízos".

[682] "O invasor não visa lucro imediato, mas pode ser visto como um *expert* e, mais tarde, ser contratado por grandes empresas de segurança ou montar ele mesmo sua empresa", ao mesmo tempo que procura ser respeitado dentro da comunidade.

[683] "Quando os invasores atacam empresas ou *sites* com a intenção de fazer manifestação política ou social".

[684] Nesta atividade encontramos o "trabalho do *hacker* ético e o trabalho do *cracker*. No caso do ético, ele utiliza a sua experiência em invasão para proteção dos sistemas das empresas que os contratam. No caso do *cracker*, usa o seu conhecimento para fazer chantagem ou espionagem entre empresas, que lhes pagam para atacar os sistemas das concorrentes."

[685] "A segurança periférica continua a ser imprescindível, mas tem sido complementada com novos meios tecnológicos, concetuais e organizacionais, que permitem uma nova abordagem." PINTO – ***Op cit.*** p. 12.

[686] "O acesso direto a estas por um utilizador qualquer ou um sistema, só é possível, após terem sido reconhecidos nas camadas exteriores, em que estão embebidas regras de proteção e acessos, políticas de segurança, processos de negócio, recuperação de dados e continuidade de funcionamento, conjugados com análises de risco em todas as fases dos processos." *Ibidem*.

[687] Comando e Controlo.

[688] PINTO – ***Op cit.*** p. 12.

[689] O conceito CERT foi pioneiro em 1988 na *Carnegie Mellon University*, nos Estados Unidos. Na altura, os seus investigadores concluíram que um número crescente de intrusões de rede exigia uma equipa de resposta de emergência centralizada, para lidar diretamente com ameaças em tempo real. Estas equipas são constituídas por ciberespecialistas e detêm meios que lhes permitem monitorizar a internet ou uma rede de dados

Assim, "estes centros tem-se constituído como autênticos provedores de serviços de segurança, incluindo não só os serviços de prevenção, tais como alertas e avisos de segurança, mas também treino de equipas, serviços de gestão de acidentes informáticos, recuperação de desastres, continuidade de negócio ou avaliação de produtos informáticos, estabelecendo acordos que lhes permitem adquirir conhecimentos e troca de informação técnica, de forma a responder com maior eficácia"[691].

específica e reagir a um ciberataque ou uma ameaça informática, em coordenação com outros CERT. Atualmente, os Estados e as organizações, como forma de melhorar a sua reação às ciberameaças, têm desenvolvido as suas Capacidades de Resposta a Incidentes de Segurança Informáticos (CRISI) constituídos por equipas de resposta imediata, em alguns casos com a designação genérica de CERT, que se têm revelado como uma forma mais eficaz de combater os ciberataques. Os CERT podem ser agrupados por vários setores: académicos, comerciais, governamentais, empresariais, militares, entre outros. Os CERT militares, estão também associados às infraestruturas críticas e ao CNCS, com o qual deverão estar profundamente coordenados de forma a maximizarem a capacidade de resposta, em situações mais graves. PINTO – ***Op cit.*** p. 13.

[690] PINTO – ***Op cit.*** p. 12.

[691] PINTO – ***Op cit.*** p. 13.

3. Enquadramento do Uso da Força: Ciberespaço

3.1. Enquadramento do Uso da Força

O presente trabalho tem como objetivo debruçar-se sobre a aplicação do uso da força no ciberespaço.

Assim, comecemos por enquadrar que este tipo de conflitos é regulado pelo Direito Internacional Público (DIP), o qual se pode definir como sendo "o conjunto de normas jurídicas criadas pelos processos de produção jurídica próprios da Comunidade Internacional, e que transcendem o âmbito estadual"[692]. Ou seja, são as regras e princípios que lidam com a conduta de Estados e de organizações internacionais, assim como de algumas das suas relações com indivíduos.

Nesta perspetiva, o interesse dos Estados no Direito Internacional passa pelos fatores de previsibilidade e legitimidade.

Os Estados têm objetivos de justiça, segurança e bem-estar. De igual modo, estes têm como direitos associados, a exclusividade da competência, a autonomia e a plenitude.

Cada Estado assume uma Personalidade Jurídica Internacional, a qual lhe confere alguns poderes[693], a saber: "*jus tractum*"; "*jus legationis*"; "*jus belli*"; e direito de reclamação internacional. Como obrigações os Estados têm que respeitar a soberania dos outros Estados e o Direito Internacional, bem como abster-se de recorrer à ameaça ou ao emprego do uso da força.

No que concerne a Portugal, e no respeito pela legalidade democrática prevista na CRP, recorde-se que o Estado Português só pode usar a força dentro dos limites internacionais aplicáveis, isto é, em situações de legítima defesa.

3.1.1. Enquadramento Internacional do Uso da Força

A ideologia tradicional do DIP até à Primeira Guerra Mundial assumia o conceito de "guerra" como um facto consensual, entre dois ou mais Estados, que se reconheciam "em estado de beligerância, a partir de um momento claro de início formal de hostilidades (declaração expressa ou implícita de guerra) e que duraria até outro momento formal, de

---

[692] PEREIRA, André; QUADROS, Fausto – **Manual de DIP.** 3ª Ed. Coimbra: Almedina, 1997. p. 31.

[693] "O poder de um indivíduo é a capacidade de fazer, mas, antes de tudo, é a capacidade de influir sobre a conduta ou os sentimentos dos outros indivíduos. No campo das relações internacionais, poder é a capacidade que tem uma unidade política de impor a sua vontade às demais". ARON, Raymond – **Paz e Guerra entre as Nações.** 2ª Ed. Brasília: Editora Universidade de Brasília, 1986. p. 99. Assim, o "poder é o produto de recursos materiais (*tangible*) e imateriais (*intangible*), que se integram à disposição da vontade política do agente, e que este usa para influenciar, condicionar, congregar, vencer, o poder de outros agentes que lutam por resultados favoráveis aos seus próprios interesses". MOREIRA, Adriano – **Teoria das Relações Internacionais.** 4ª Ed. Coimbra: Almedina, 2002. p. 247.

reconhecimento recíproco de uma situação pós-bélica, formalizado com um tratado de paz"[694]. Como tal, poderemos assumir que "as regras sobre o denominado "*jus belli*" ou direito da guerra são antigas e foram elaboradas na assunção de haver uma nítida separação entre um tempo de paz e um tempo de guerra"[695].

Todavia, a sua evolução levou a que o tema do uso da força no Direito Internacional manifeste uma maior complexidade do que uma abordagem mais superficial possa apontar. Tal assenta no facto de o Direito Internacional constituir "a base normativa delimitativa da licitude do uso da força"[696]. Contudo, refira-se que este paradigma tem levantado algumas questões, fator que tem contribuído para a sua evolução, "por vezes resultante de uma fragilização, e consolidação deste ramo do direito"[697], tendo tido como resultado prático desafiar os próprios preceitos do Direito Internacional.

Historicamente, assistimos a conceções e abordagens diferentes desta temática, a qual se alicerça na própria evolução do Direito Internacional no que concerne à autoridade de uma ordem jurídica internacional.

Neste sentido, não poderemos deixar de assinalar a "influência de Hugo Grócio, considerado o fundador do DIP que, na sua obra *De iure belli ac pacis*, de 1625, estabeleceu contornos formalistas de recurso à guerra (*ius ad bellum*) e regras orientadoras dos conflitos armados (*ius in bello*) no âmbito da conceção de guerra justa. A paz de Westfália de 1648 e a consequente emergência da figura do Estado soberano marca o início do Direito Internacional clássico"[698]. Aqui, o recurso ao uso da força para imposição dos interesses estatais levou ao consolidar do conceito de "soberania". Em complemento, registe-se que nesta época "nem vigorava um direito expresso nem uma proibição geral de uso da força. Na verdade, existia uma "indiferença" material por parte do direito que se verificou até à Primeira Guerra Mundial"[699].

---

[694] SARAIVA, Rodrigo – **Legítima Defesa ou Represália? O uso da força no conflito armado de 2001 no Afeganistão.** São Paulo: Universidade de São Paulo, Faculdade de Direito, 2009. Dissertação de Mestrado. p. 44.
[695] *Ibidem*.
[696] SANTOS, Sofia – **O uso da força no direito internacional e os desafios ao paradigma onusiano.** Belo Horizonte: Revista da Faculdade de Direito da Universidade Federal de Minas Gerais. N.º 61, Julho-Dezembro, 2012. p. 534.
[697] Esta conexão é visível a vários níveis, dado que o quadro jurídico-normativo nesta matéria vincula os Estados, principais sujeitos jurídicos, as organizações internacionais, e afeta, igualmente, o indivíduo e entidades não-estatais, sendo que estas, apesar de não reunirem consenso sobre a sua qualidade jurídica, têm adquirido um crescente significado nas relações internacionais. *Ibidem*.
[698] SANTOS – ***Op cit.*** 2012. p. 535.
[699] *Ibidem*.

Com efeito, a criação da Organização das Nações Unidas (ONU) a 26 de junho de 1945 na Conferência de São Francisco veio significar uma mudança de paradigma no que respeita à instituição de parâmetros jurídico-internacionais relativos ao uso da força, tendo por base um sistema jurídico de índole universal.

Este sistema tinha como desiderato "colmatar os erros e as lacunas das tentativas anteriores que se revelaram incapazes de instituir uma norma proibitiva do uso da força de natureza internacional e universal e de impedir o início da Segunda Guerra Mundial: a Sociedade das Nações, em 1919, cujo pacto contemplou uma moratória de guerra e do Pacto Briand-Kellog, em 1928, que estabeleceu uma renúncia ao uso da força, exceto no caso de legítima defesa"[700].

Deste modo, a ONU apresenta-se como uma organização de fins gerais, tal é a vastidão das atribuições que lhe foram confiadas, sendo de salientar entre os seus objetivos o de garantir a paz e a segurança internacionais, bem como a codificação do Direito Internacional e a realização de todas as ações comuns que sirvam àqueles objetivos. No âmbito dos seus princípios salientemos: o princípio da resolução pacífica dos conflitos internacionais, e o princípio da proibição geral do uso da força nas relações internacionais[701].

Nesta perspetiva, surge então a Carta das Nações Unidas (CNU)[702], a qual representou a "cristalização de um quadro normativo que se tinha vindo a desenvolver no Direito Internacional costumeiro, assente na recusa de um caráter arbitrário do uso da força"[703]. Quanto ao "*jus ad bellum*", as fontes importantes das normas do DIP, tais como os usos e costumes internacionais, "não tiveram qualquer relevância na regulamentação dos conflitos, então regulados unicamente pelas normas da CNU, [pelo que] há outras manifestações

[700] *Ibidem*.
[701] "Se o sistema universal de segurança coletiva proíbe o uso ou ameaça do uso da força pelos Estados, e lhes impõe o dever de resolverem as suas controvérsias internacionais por meios pacíficos, em contrapartida, a ONU, através dos seus órgãos, deverá zelar pela manutenção da paz e segurança internacionais, exercendo ou autorizando o uso da força armada", quando necessário para cumprir esse fim. SARAIVA – ***Op cit.*** p. 49.
[702] Refira-se que já no seu preâmbulo, a CNU veio fixar a preservação das "gerações vindouras do flagelo da guerra que por duas vezes, no espaço de uma vida humana, trouxe sofrimentos indizíveis à humanidade". De igual modo, o seu n.º 1 do art.º 1.º define como objetivo desta Carta "manter a paz e a segurança internacionais e para esse fim tomar medidas coletivas eficazes para prevenir e afastar ameaças à paz e reprimir os atos de agressão, ou outra qualquer rutura da paz e chegar, por meios pacíficos, e em conformidade com os princípios da justiça e do Direito Internacional, a um ajustamento ou solução das controvérsias ou situações internacionais que possam levar a uma perturbação da paz". ESCARAMEIA, Paula – **Guerra do Iraque – Fundamentos Jurídicos do Uso da Força.** Lisboa: Instituto Superior de Ciências Sociais e Políticas, Universidade Técnica de Lisboa, 2003. p. 1.
[703] SANTOS – ***Op cit.*** 2012. p. 536.

normativas que consagram o mesmo direito e, portanto, reafirmam as limitações que o DIP impõe, na atualidade, ao "*jus ad bellum*" dos Estados, por mais poderosos que sejam"[704].

A CNU define alguns pontos de apoio, o que designa por princípios que são sumariamente: o princípio da igualdade soberana dos EM; o princípio do dever da boa fé no cumprimento das obrigações; o princípio da resolução pacífica dos conflitos internacionais; o princípio da proibição do uso da força nas relações internacionais; entre outros.

A referida proibição geral do uso da força assume-se como um princípio geral e basilar da organização mundial, o qual surge apenas com o art.º 2º n.º 4 da CNU, que afirma: "A Organização e os seus membros, para a realização dos objectivos do artigo 1º, agirão de acordo com os seguintes princípios: (…) 4) Os membros deverão abster-se nas suas relações internacionais de recorrer à ameaça ou ao uso da força[705], quer seja contra a integridade territorial ou a independência política de um Estado, quer seja de qualquer outro modo incompatível com os objectivos das Nações Unidas (NU)[706]". Este artigo é um indicador daquilo que é o desiderato da CNU, a qual se alicerça na necessidade da paz mundial, como é manifesto no seu primeiro artigo.

O Direito Internacional consuetudinário veio consolidar o art.º 2.º n.º 4 da CNU como uma norma irrefutável de "*jus cogens*[707]", isto é, uma norma imperativa que, no dizer do art.º 53.º da Convenção de Viena sobre Direito dos Tratados de 1969 "… é a que for aceite e reconhecida pela comunidade internacional dos Estados no seu conjunto como norma à qual nenhuma derrogação é permitida e que só pode ser modificada por uma nova norma de Direito Internacional geral com a mesma natureza", tendo, por isso, uma força acrescida, reconhecida por toda a comunidade internacional.[708]Ou seja, a mesma "constitui uma norma imperativa de direito internacional geral da qual nenhuma derrogação é permi-

[704] SARAIVA – ***Op cit.*** p. 50.
[705] Constate-se ainda que, o termo "guerra" não é explicitado de forma expressa, tendo-se optado pela expressão "ameaça ou uso da força", a qual é mais "abrangente e atual, e, portanto, menos suscetível à interpretação restritiva". SARAIVA – ***Op cit.*** p. 53.
[706] Segundo este art.º, os membros da ONU devem-se coibir de recorrer à ameaça ou ao uso da força contra a integridade territorial ou a independência política de qualquer Estado, como forma preventiva de quebrar a paz alcançada. SARAIVA – ***Op cit.*** p. 52.
[707] O "*jus cogens*" é a "locução latina que significa direito taxativo, ou seja, o conjunto de normas inderrogáveis mediante consentimento das partes e que não admitem pacto contrário dada a natureza do bem que tais normas tutelam: a ordem pública. A estas normas que são designadas por imperativas, opõem-se outras que dependem da vontade das partes, ou seja, as normas dispositivas." O art.º 53º da Convenção de Viena define a norma de "jus cogens" como "a que for aceite e reconhecida pela comunidade internacional dos estados no seu conjunto como norma à qual nenhuma derrogação é permitida e que só pode ser modificada por norma de Direito Internacional da mesma natureza". Cfr. **Dicionário Diplomático.** [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://dicionariodiplomatico.blogspot.pt/2003/11/j.html.
[708] ESCARAMEIA – ***Op cit.*** p. 1.

tida, e que só pode ser modificada por nova norma de direito internacional da mesma natureza"[709], uma vez que regulam e asseguram direitos fundamentais dos indivíduos[710].

Com efeito, a fundação da ONU veio preconizar através da ordem jurídica internacional a proibição do uso da força, ao abrigo do art.º 2.º n.º 4[711] da CNU, a qual não é passível de quaisquer tipos de interpretações[712]. A controvérsia que acaba por se colocar é com a interpretação extensiva das exceções no que diz respeito às circunstâncias do exercício do direito à legítima defesa, de acordo com o seu art.º 51.º[713], tal como veremos mais à frente.

Em complemento, refira-se que, quando "a norma contida no art.º 2º n.º 4 da CNU vincula a ameaça do uso da força à independência política de outro Estado, significa dizer que proíbe a coerção militar para direcionar ou restringir a independência do Estado em escolher e gerir o seu próprio sistema político, social, cultural e económico, bem como a sua política externa". Contudo, este impedimento generalizado da ameaça ou uso das FA nas relações internacionais, não é estanque, uma vez que a CNU prevê as seguintes exceções: "a) no exercício da legítima defesa individual ou coletiva; b) nas ações coletivas para a manutenção da paz; c) na luta dos povos no quadro do exercício de seu direito à autodeterminação; e d) nas intervenções coletivas por motivos humanitários ou de humanidade"[714]. Por outras palavras, os EM da ONU nas suas relações internacionais estão legitimados a "recorrer à ameaça ou ao emprego da força contra a integridade territorial ou a independência política de quaisquer outros Estados, desde que as hipóteses contempladas pela CNU assim os autorizem, e desde que sejam respeitadas as condições para a aplicação das regras que lidam com as exceções à regra fundamental, que é a proibição do uso potencial ou atual da força"[715].

---

[709] SARAIVA – ***Op cit.*** p. 53.
[710] A CNU entra no ordenamento jurídico português através do art.º 8.º, n.º 1 da CRP, pois esta é uma norma "*jus cogens*". A Convenção de Viena aplica-se aos Estados, entrando no ordenamento jurídico português através do art.º 8.º n.º 1 CRP, pois esta Convenção traduz normas "*jus cogens*"no tocante a regras costumeiras de elaboração dos Tratados.
[711] "Todos os membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a independência política de qualquer Estado, ou qualquer outra ação compatível com os propósitos das Nações Unidas."
[712] "Pelo menos desde a fundação da ONU em 1945, o sistema jurídico internacional preconizou a proibição explícita do uso da força, notadamente no art.º 2.º n.º 4.º da CNU. Esta norma central da CNU e a sua equivalência no direito internacional costumeiro proíbem os Estados de utilizarem a força de caráter militar, mesmo se o governo de um Estado não tiver sido reconhecido internacionalmente. Esta interpretação do art.º 2.º n.º 4.º da CNU é incontestável: a controvérsia diz respeito às exceções, nomeadamente as circunstâncias em que o direito à legítima defesa nos termos do art.º 51.º da CNU pode ser exercido." SARAIVA – ***Op cit.*** p. 43.
[713] *Ibidem*.
[714] SARAIVA – ***Op cit.*** p. 54.
[715] *Ibidem*.

Por outro lado, atualmente verifica-se uma contraposição entre o direito internacional clássico e o contemporâneo. Se no primeiro era admissível o uso de força por qualquer Estado ou aliança de Estados e não se concebia o uso de força por parte da comunidade internacional, já no segundo o uso da força é exceção e prevalece o uso da força pela comunidade internacional. Assim, tudo se passa hoje como se o Conselho de Segurança (CS) das NU se arrogasse do monopólio do uso força[716], uma vez que este sistema centralizou a prerrogativa do uso da força numa entidade distinta dos seus sujeitos: a ONU.

Com efeito, registemos que o Direito Internacional impõe as suas normas sobre os Estados que as violam, desde as regras para a resolução pacífica das controvérsias[717], em algumas já com um papel superior e decisivo do CS, como nos casos dos artigos 34.º, 36.º e 38.º da CNU. Mas esta resolução poderá ir mais longe podendo o Direito Internacional ser imposto com recurso à força conforme previsto no Capitulo VII, o qual se refere às Ações em caso de ameaça à Paz, rutura da Paz e ato de agressão.

Deste modo, "as normas jurídicas, que constituem o arcabouço normativo da ONU são as únicas que, na atualidade, legitimam o emprego virtual ou real da força militar nas relações internacionais; além de elas provirem de uma verdadeira delegação de poderes que os Estados fizeram à ONU, as decisões desta organização têm sido consideradas, por várias outras fontes normativas, como integradas no poderoso arcabouço dos usos e costumes internacionais que abrigam todos os povos na atualidade"[718].

A CNU concretiza os sinais de compromisso internacionais por todo o seu corpo, sendo um dos traços mais vincados desta efetivação o disposto nos art.º 92.º e seguintes, e respetivo anexo onde se encontra estabelecido o estatuto do Tribunal Internacional de Justiça (TIJ), o qual poderá ser adotado não só pelos países da organização, mas também por outros em condições especiais conforme discorre o art.º 93.º.

Neste contexto, importa aqui abordar a problemática da responsabilidade penal internacional. Assim, o "Direito Internacional Penal corresponde ao sistema de princípios e normas do DIP que descreve os crimes internacionais de aplicação de sanções internacionais"[719], o qual procura punir os sujeitos que tenham infringido os mais altos valores protegidos pelo DIP sujeitando-os a penas de prisão por terem cometido crimes internacionais,

[716] Artigos 24.º e 28.º da CNU.
[717] A solução pacífica de controvérsias está presente no capítulo VI da CNU.
[718] SARAIVA – ***Op cit.*** p. 42.
[719] GOUVEIA, Jorge – **Direito Internacional Penal, Uma perspetiva dogmático crítica.** Coimbra: Almedina Editora, 2008. ISBN 9789724035932. p. 65.

uma vez que se trata de uma responsabilidade individual, que recai sobre as pessoas por atos criminalmente puníveis e não da responsabilidade dos Estados.

No que concerne ao Direito Internacional Penal, importa aqui distinguir o Tribunal Internacional de Justiça e o Tribunal Penal Internacional (TPI).

Assim, o TIJ é o principal órgão judicial das NU que tem como função resolver controvérsias entre Estados, emitindo pareceres consultivos sobre qualquer questão jurídica, mediante solicitação da Assembleia do CS ou de outros órgãos ou organizações especializadas, de acordo com o art.º 96º e art.º 65º e seguintes do presente Estatuto. Os pareceres emitidos não têm caráter vinculativo, mas possuem considerável valor político. O seu funcionamento é regulado pelo Estatuto que é parte integrante da CNU, constantes no art.º 92º; porém, este facto não significa que todos os EM se encontram sujeitos à sua jurisdição, dependendo esta de uma declaração de aceitação de acordo com o art.º 36º n.º 2.

Já o TPI[720], sediado em Haia, foi criado pelo Estatuto de Roma em 1998, obtendo 60 ratificações e entrando em vigor em 2002. O mesmo tem como função apreciar a responsabilidade direta ou indireta das pessoas que estiveram envolvidas na prática dos crimes internacionais, dando um sinal à comunidade de que os autores de graves crimes internacionais, isto é, violações do Direito Internacional Humanitário (DIH), não passem sem punição. Em 2016, o TPI era composto por 124 Estados partes, existindo vários Estados que assinaram o estatuto mas ainda não ratificaram como é o caso dos Estados Unidos e da China, e muito recentemente a Rússia, entre outros. A assinatura do Estatuto é uma mera declaração de intenção, daí que, só após a ratificação, ou seja, inclusão no direito interno e respetiva publicação no próprio Estado é que passa a ser vinculativo. Os atos cometidos por cidadãos de Estados que fazem parte do TPI em Estados que não fazem parte, são também apreciados pelo TPI.

O TPI rege-se por importantes princípios: o princípio do *ne bis in idem* – proibição da dupla condenação (art.º 20.º); princípio da presunção da inocência do arguido (art.º 66.º); princípio da irrelevância das imunidades dos arguidos (art.º 27.º); princípio da cooperação com o tribunal (art.º 86.º e seguintes); o princípio do *nullum crimen sine lege* ao prever que nenhuma pessoa poderá ser criminalmente responsabilizada pela sua conduta quando esta não constitua, no momento que tiver lugar, um crime de competência.

[720] O TPI nasce, na realidade, como resultado de um longo processo de reconhecimento da necessidade de responsabilizar criminalmente indivíduos que atentassem de forma grave certos direitos humanos básicos, sendo que até à sua criação foram várias as instituições judiciárias internacionais criadas, bem como Tribunais *ad hoc*, criando pela primeira vez um tribunal penal permanente.

Recordemos que, o Estatuto de Roma reconheceu a existência de valores comuns como a paz, a segurança e o bem-estar da Humanidade que deveriam ser salvaguardados pelo TPI. O preâmbulo do Estatuto consagra a noção de "crimes mais graves", aqueles que afetam a comunidade internacional no seu conjunto e que se encontram também enunciados no art.º 5.º: o crime de genocídio[721], os crimes contra a humanidade[722], os crimes de guerra[723], e o crime de agressão[724]. O direito de punir estes tipos de crimes passou para a esfera internacional (*jus puniendi*), o que até então a punição e a sua inobservância dependia exclusivamente das jurisdições penais nacionais[725].

O Estatuto de Roma[726], ao tipificar os Crimes de Guerra, contribui desse modo para assegurar a eficácia dos instrumentos do Direito Internacional Humanitário.

Todavia, o TPI apresenta alguns limites[727], tais como, o Estatuto não vir a ser de jurisdição universal e que seja vinculativa aos Estados; a relação com o CS (interferência

[721] O art.º 6º consagra o crime de genocídio, tratando-se de qualquer ato praticado com intenção de destruir, no todo ou parcialmente, um grupo nacional, étnico, rácico ou religioso: homicídio e ofensas à integridade física ou mental dos membros, sujeição intencional do grupo a condições de vida pensadas com a finalidade de provocar a sua destruição física, total ou parcial, imposição de medidas destinadas a impedir os nascimentos no seio desse grupo e a transferência, forçada, de crianças para um outro grupo.

[722] O art.º 7º que define os crimes contra a humanidade como qualquer ato cometido no quadro de um ataque generalizado ou sistemático contra a população civil com conhecimento desse ataque, como por exemplo: homicídio, extermínio, escravidão, deportação ou transferência forçada, prisão em violação das normas fundamentais do Direito Internacional, tortura, violação, escravatura sexual, perseguição de um grupo ou coletividade que possa ser identificado, por motivos políticos, raciais, nacionais, éticos, culturais, religiosos ou de sexo ou em função de outros critérios aceites universalmente, desaparecimento forçado de pessoas, crime de apartheid e outros atos desumanos de natureza semelhante que provoquem intencionalmente considerável sofrimento, ferimentos graves ou afetem a saúde mental ou física.

[723] O art.º 8º refere os Crimes de Guerra prescritos nas Convenções de Genebra de 1949, particularmente "quando cometidos como parte integrante de um plano ou de uma política ou como parte de uma prática em larga escala", os quais desde a sua origem o DIH procurou regular – conflitos entre Estados no âmbito do Direito Internacional, regulando também casos no âmbito de conflitos armados que não sejam de caráter internacional.

[724] O crime de agressão foi definido na conferência de Kampala, onde a responsabilidade criminal é somente atribuída a indivíduos que se encontrem numa posição de efetivamente exercer controlo e dirigir uma ação política ou militar de um Estado, o qual consiste num ato de agressão de um Estado contra a soberania de outro Estado através do uso da força armada ou de outro modo incompatível com os princípios da Carta. De realçar que o ato de agressão tem que ser analisado no contexto do seu "caráter", "escala" e "gravidade", em que somente se pode verificar um crime de agressão quando um ato de agressão constitui uma manifesta violação da Carta. Assim, embora o ato de agressão possa ser cometido apenas por um Estado, a responsabilidade por tais atos ilícitos reside no indivíduo que é responsável por tal ação estatal.

[725] Este sistema punitivo assenta no princípio da complementaridade (art.º 1.º), a fim de complementar as jurisdições penais internacionais, o qual ainda que constrangendo o poder do Tribunal, lhe permite exercer influência na esfera estatal. O Tribunal é competente para determinar a inexistência de vontade de agir por parte de um Estado, nos seguintes casos: situações em que se comprove que o processo noutro Tribunal foi instaurado ou se encontra pendente ou a decisão foi proferida com o propósito de subtrair à Pessoa a responsabilidade por crimes da sua competência, ter havido demora injustificada no processamento ou processo não ter sido ou não estar a ser conduzido de modo independente ou imparcial, e ter estado ou se encontrar a ser conduzido de maneira incompatível com intenção de fazer responder a pessoa em causa perante a justiça (art.º 17.º n.º 2).

[726] O Estatuto preceitua a obrigação de todos os Estados partes cooperarem com o tribunal no inquérito e no procedimento criminal (art.º 86.º) e de adotarem no Direito interno procedimentos que permitam responder a todas as formas de cooperação internacional e auxilio judiciário previsto (art.º 88.º).

de um órgão político num órgão jurisdicional); quando o Estado não faz parte, mesmo que os atos tenham sido cometidos por cidadãos não abrangidos; inexistência de um mecanismo que assegure a responsabilização/implementação das decisões, nomeadamente a execução dos mandados de detenção.

Voltando à problemática do uso da força no DIP, e de acordo com a CNU, o Conselho de Segurança das NU tem um papel vital, uma vez que "não partilha esse poder com nenhum outro órgão, num sistema de segurança coletiva e pública"[728], considerando que o CS se assume como "o órgão central da ONU, competindo-lhe essencialmente ser o guardião da paz e da segurança internacionais"[729].

Como tal, o CS das NU assume o inerente procedimento sancionatório, o qual é diversificado e comporta diversos momentos, de entre eles se destacando: a iniciativa; a apreciação; e a decisão. De qualquer maneira, esta é "uma intervenção intensamente sujeita a vários princípios de tipo procedimental e material, de que cumpre naturalmente evidenciar o princípio da proporcionalidade"[730].

Quanto às sanções, com o desígnio de se evitar ou de se reprimir uma situação de rotura da paz e da segurança internacionais, poderemos referir que as sanções aplicáveis se dividem em sanções coativas militares e não militares[731].

Desta forma, verificamos que existem diversas medidas coercitivas militares, as quais estão na autoridade do CS das NU[732].

---

[727] Acrescente-se que se verifica a necessidade, no âmbito da jurisdição internacional, de um TPI permanente, o qual ainda transporta consigo virtudes e fragilidades, tais como a oposição da maior parte das grandes potências militares do planeta (EUA, China, Rússia, Irão, entre outros) e também a sua reduzida amplitude de ação, a sua "africanização" (visto a pendência dos processos situar-se no continente africano) e a incapacidade de ter acesso a arguidos com poder político significativo.

[728] GOUVEIA, Jorge – O uso da força no DIP. In **Revista Brasileira de Estudos Políticos.** N.º 107. Belo Horizonte: 2013. (julho/dezembro). p. 163.

[729] "Nesta matéria o CS tem poder exclusivo, sob duas vertentes: externamente, porque nenhuma outra instância se pode arrogar do exercício de poderes de manutenção da paz internacional, sendo esta uma incumbência só atribuída à ONU, o que não belisca os acordos de legítima defesa coletiva, que se lhe subordinam; e internamente, porque nenhum outro órgão pode intervir, o que a acontecer é sempre por impossibilidade ou a mando do CS, cabendo-lhe mesmo a execução das decisões do Tribunal Internacional de Justiça, apenas a Assembleia Geral podendo excecionalmente intervir no caso de paralisação do CS."

[730] GOUVEIA – ***Op cit.*** 2013. p. 166.

[731] Naturalmente, entre estas é estabelecido "um apurado sentido de proporcionalidade, só se justificando a aplicação ou a passagem às medidas mais drásticas no caso de outras medidas mais suaves não surtirem igual efeito. Para além disso, ainda se admite que o CS adote um procedimento provisório, podendo intercalarmente propor medidas temporárias. A fim de evitar que a situação se agrave, o CS poderá, antes de fazer as recomendações ou decidir a respeito das medidas previstas no art.º 39.º, instar as partes interessadas a aceitar as medidas provisórias que lhe pareçam necessárias ou aconselháveis". GOUVEIA – ***Op cit.*** 2013. p. 169.

[732] O CS das NU exerce a sua autoridade na implementação de medidas coercitivas militares, quando, por exemplo, se verifica a necessidade da execução de operações militares robustas para a manutenção ou restabelecimento da paz, mediante a natureza de determinados conflitos. Por outras palavras, falamos de "missões compostas por forças fortemente militarizadas, destacadas sem o consentimento das partes, com base num

Por este motivo, acompanhamos a ideia de necessidade de ser realizada uma reforma do quadro institucional, a qual deverá "ocorrer em concomitância com uma reinterpretação do quadro normativo. (…) Esta reinterpretação deve estar plasmada numa resolução, na qual o CS prescreva os princípios referentes ao recurso ao uso da força coletiva ao abrigo do Capítulo VII e no âmbito do direito de legítima defesa coletiva nos termos do art. 51º, limites jurídicos a este recurso no processo de imposição de medidas coercitivas militares bem como a dimensão e tipologia das FA requeridas"[733].

No que respeita ao recurso ao uso da força coletiva ao abrigo das medidas previstas no Capítulo VII da CNU, importa aclarar que o mesmo assume como pressuposto capital a verificação de que está ocorrendo uma qualquer ameaça à paz, rotura da paz ou ato de agressão[734].

Por outro lado, em alternativa, poderemos aplicar sanções coativas não militares ou bélicas, mesmo que assumam um caráter coercivo, devido a serem obrigações e não recomendações. Ainda assim, as mesmas não envolvem o uso da força e a CNU avança com alguns exemplos de sanções: "a interrupção, completa ou parcial, das relações económicas; a interrupção, completa ou parcial, dos meios de comunicação ferroviários, marítimos, aéreos, postais, telegráficos, radioelétricos, ou de qualquer outra natureza; e o rompimento das relações diplomáticas"[735].

Em relação às sanções coativas militares, o uso da força armada pressupõe, de acordo com a CNU, uma cláusula geral com estes termos: "poderá levar a efeito, por meio de forças aéreas, navais ou terrestres, a ação que julgar necessária para manter ou restabelecer a paz e a segurança internacionais"[736].

---

mandato do Conselho e que podem recorrer ao uso da força para além do exercício do direito de legítima defesa previsto no art.º 51º da Carta com o objetivo, por exemplo, de impor acordos de paz, fazer cumprir o respeito por sanções impostas e conduzir operações militares contra um Estado invasor". SANTOS, Sofia – **Reforma dos Instrumentos Militares e da Autoridade do CS das Nações Unidas na Implementação de Medidas Coercitivas Militares**. Janus.net, e-journal of International Relations, OBSERVARE. Vol. 4. N.º 1. 2013. p. 8.

[733] SANTOS – ***Op cit.*** 2013. p. 13.

[734] Percebe-se que este endurecimento das medidas não acontece apenas na deflagração de um conflito armado, mas pode surgir dentro de uma ótica preventiva desse mesmo conflito. A aplicação dessas medidas é, contudo, encarada sempre com gradualismo, uma vez que pode ser antecedida da formulação de recomendações com o propósito de ser evitada ou de ser feita cessar a situação de rotura, a fim de manter ou restabelecer a paz e a segurança internacionais. GOUVEIA – ***Op cit.*** 2013. p. 170.

[735] *Ibidem*.

[736] *Ibidem*.

Esta cláusula geral será posteriormente classificada em "duas operações militares, nos três ramos possíveis das FA, que a integram e que são: as demonstrações; e os bloqueios"[737].

Acrescente-se que, o "uso da força militar pode ser feito diretamente pelos Estados, sendo autorizados a tanto, ou por forças da ONU, embora até ao momento este quadro próprio nunca tenha sido constituído"[738].

Com efeito, poderemos então concluir que o CS, de acordo com o n.º 1 do art.º 7.º da CNU, se constitui como o principal órgão com a responsabilidade na manutenção da paz e da segurança internacionais. Para tal faz uso dos seus poderes de adoção de soluções pacíficas de controvérsias, na execução de ações em caso de ameaça à paz, rutura da paz ou em atos de agressão, celebração de acordos regionais e a imposição de um regime internacional de tutela, previstos nos capítulos VI, VII, VIII e XII da Carta. Ao abrigo do capítulo VI (solução pacífica de conflitos), mas sobretudo do capítulo VII, o CS adquire uma ampla capacidade de ação com vista à concretização da sua responsabilidade primária de manutenção da paz e segurança internacionais.

Nesta perspetiva, acrescente-se que, a legalidade do uso da força só se verifica numa situação de legítima defesa e com a autorização do CS, para determinar as medidas a implementar com ou sem o recurso ao uso da força, nos termos do art.º 41.º da CNU. Todavia, o uso da força é sempre precedido da procura da solução pacífica de qualquer conflito, de acordo com o capítulo VI da CNU.

Assim, aquando da deteção de uma controvérsia, pode a ONU convidar as partes em conflito a encontrar soluções por intermédio de negociação, inquérito, mediação, conciliação, arbitragem, via judicial, recurso a organizações ou acordos regionais, ou qualquer outro meio pacífico à sua escolha, de acordo com o art.º 33.º da CNU.

Igualmente, pode o CS por sua iniciativa investigar qualquer controvérsia ou situação suscetível de provocar atritos entre as Nações ou de dar origem a uma controvérsia, a fim de determinar se a continuação de tal controvérsia ou situação pode constituir ameaça à manutenção da paz e da segurança internacionais, nos termos do art.º 34.ºda CNU.

---

[737] Naturalmente que estas duas categorias não se referem à utilização mais óbvia da força armada, que é o uso da força através da ocupação física do Estado prevaricador, com tudo quanto isso implica nos atos que se impõem para restabelecer a legalidade internacional. GOUVEIA – ***Op cit.*** 2013. p. 171.

[738] Por outro lado, é também aceite "que as organizações regionais sejam chamadas a colaborar na manutenção da paz e segurança internacionais, dizendo que o CS utilizará, quando for caso disso, tais acordos e organizações regionais para uma ação coercitiva sob sua própria autoridade".GOUVEIA – ***Op cit.*** 2013. p. 172.

Por seu lado, nos casos onde existe uma vontade negocial entre os Estados envolvidos numa controvérsia e os mesmos não a consigam resolver pelos seus próprios meios, poderão estes submetê-la ao CS (art.º 37.ºda CNU), sendo que o CS se irá guiar pelos procedimentos previstos no art.º 36.ºda CNU.

Desta forma, podemos concluir que a ONU, como um organismo com uma forte capacidade de influência, assume um papel preponderante na prevenção e mediação de divergências entre os Estados, optando sempre por uma solução de negociação.

O conceito estratégico da OTAN de Lisboa em 2010 cimentou os desenvolvimentos institucionais e concetuais ocorridos na primeira década do século XXI e delimitou a orientação futura, permanecendo o objetivo principal de salvaguardar a liberdade e segurança de todos os seus membros através de meios políticos e militares. Na prática, este conceito estratégico de Lisboa reafirma a missão de "salvaguardar a liberdade dos seus povos, a sua herança comum e a sua civilização, fundadas nos princípios da democracia, das suas liberdades individuais e pelo respeito do direito"[739] (art.º 1.º e seguintes).

Nesta perspetiva, a OTAN identifica como ameaças: a proliferação de mísseis balísticos e de armas nucleares; o terrorismo e o uso de armas nucleares, biológicas e químicas por grupos extremistas; o tráfico de armas, de droga e de seres humanos; os ciberataques; as ameaças à segurança energética e ao abastecimento energético; as alterações climáticas, a escassez de água e a escassez energética.

Voltando à problemática da proibição do uso da força, ao abrigo do art.º 2.º n.º 4 da CNU, iremos agora elencar as quatro exceções admissíveis ao uso da força:

1) O direito de legítima defesa, nos termos do art.º 51.º; neste particular, constatamos que: existe uma ausência de uma definição de "ataque armado", bem como subsiste a questão da responsabilidade do exercício de legítima defesa contra situações de terrorismo; no caso da ocorrência de um ataque armado, em que casos estaremos perante uma legítima defesa preventiva e/ou pré-emptiva; e a subordinação aos princípios da proporcionalidade, necessidade, atualidade/iminência;

2) As sanções coativas militares, ao abrigo do art.º 42.º do Capitulo VII da Carta, no âmbito do sistema de segurança coletiva[740]: "Se o CS considerar que as medidas previstas no

[739] Recorde-se que, a OTAN tem como três funções principais: a defesa coletiva (art.º 5.º), a gestão de crises (antes, durante e pós-conflito) e a segurança cooperativa (cooperação com outras organizações internacionais e outros Estados relevantes não membros).

[740] Nos termos do art.º 39º, o "CS determinará a existência de qualquer ameaça à paz, rutura da paz ou ato de agressão e fará recomendações ou decidirá que medidas deverão ser tomadas de acordo com os artigos 41º e 42º, a fim de manter ou restabelecer a paz e a segurança internacionais". O pressuposto vital para a aplicação

art.º 41.º[741] seriam ou demonstraram ser inadequadas, poderá levar a efeito, por meio de forças aéreas, navais ou terrestres, a ação que julgar necessária para manter ou restabelecer a paz e a segurança internacionais. Tal ação poderá compreender demonstrações, bloqueios e outras operações, por parte das forças aéreas, navais ou terrestres dos membros das NU";
3) As medidas adotadas por organizações regionais, ao abrigo do art.º 53.º, n.º 1: "O CS utilizará, quando for caso, tais acordos e organizações regionais para uma ação coercitiva sob a sua própria autoridade, uma vez que o CS detém o monopólio da força. Nenhuma ação coercitiva será, no entanto, levada a efeito em conformidade com acordos ou organizações regionais sem autorização do CS, com exceção das medidas contra um Estado inimigo, como está definido no n.º 2 deste artigo";
4) As medidas adotadas contra anteriores Estados inimigos[742], nos termos conjugados dos artigos 107.º e 53.º, n.º 1.

Todavia, constatamos que o paradigma onusiano revela insuficiências normativas, considerando que o "sistema jurídico-normativo não tem conseguido impedir o uso da força para além dos parâmetros delineados"[743]. Tal, assenta na questão deste sistema ter por base o modelo clássico de conflitos[744].

Por outro lado, temos ainda a questão da ingerência humanitária, a qual pode ser definida como a intervenção com recurso ao uso da força militar no território de um Estado sem o seu consentimento, por parte de um outro Estado ou Estados ou organizações internacionais com o propósito de proteger a população desse Estado de graves violações dos direitos humanos.

---

das medidas previstas no capítulo VII da CNU é o da verificação de que está a ocorrer uma "qualquer ameaça à paz, rutura da paz ou ato de agressão". Só o CS pode determinar se ocorreu uma violação do princípio de não recurso à força. Inicialmente, os Estados ameaçados ou atacados devem informar o CS de uma agressão contra a sua integridade territorial ou independência política. Além disso, outros Estados e o Secretário-Geral podem chamar ainda a atenção do CS para uma situação de ameaça ou rutura da paz ou agressão efetiva.

[741] Em relação às sanções coativas não militares, de acordo com o art.º 41º, o "CS decidirá sobre as medidas que, sem envolver o emprego de FA, deverão ser tomadas para tornar efetivas as suas decisões e poderá instar os membros das NU a aplicarem tais medidas. Estas poderão incluir a interrupção completa ou parcial das relações económicas, dos meios de comunicação ferroviários, marítimos, aéreos, postais, telegráficos, radioelétricos, ou de outra qualquer espécie, e o rompimento das relações diplomáticas".

[742] Os antigos adversários na Segunda Guerra Mundial, designadamente, o Japão, a Alemanha, e a Itália.

[743] SANTOS – ***Op cit.***2012. p. 536.

[744] "As novas ameaças, como o terrorismo internacional e a proliferação de armas de destruição maciça, bem como os conflitos intraestaduais demonstram as limitações deste sistema. (…) As divergentes interpretações, quer entre os EM quer na doutrina jusinternacionalista, relativamente à existência de uma "ameaça à paz" com base no art.º 39.º, à aplicação de medidas coercitivas militares previstas no art.º 42.º no âmbito da proteção dos direitos humanos, aos limites ao exercício do direito de legítima defesa de acordo com o art.º 51.º e, consequentemente, ao alcance da proibição do uso da força estatuída no art.º 2.º, n.º 4, têm dificultado a aplicação eficaz da Carta e a produção de segurança jurídica." *Ibidem*.

Esta teoria decorre da perceção de que perante um fenómeno conflitual de cariz intraestadual, onde se podem verificar graves violações dos direitos humanos e catástrofes humanitárias, tal como verificado na década de noventa do século XX, o princípio de soberania não se poderia sobrepor à proteção dos direitos humanos, tal como no entendimento clássico de domínio reservado. Todavia, a determinação da existência de uma "ameaça à paz" e a autorização do recurso ao uso da força, ao abrigo do Capitulo VII, para pôr termo a graves violações dos direitos humanos ficarão sempre sujeitas ao papel do CS das NU.

De igual modo, existem outros instrumentos jurídicos internacionais que se debruçam sobre a problemática do uso da força, a saber: a Declaração Universal dos Direitos do Homem (DUDH), a Convenção Europeia dos Direitos do Homem (CEDH), o Código de Conduta para os Funcionários Responsáveis pela Aplicação da Lei, e os Princípios Básicos sobre a Utilização da Força e de Armas de Fogo pelos Funcionários Responsáveis pela Aplicação da Lei.

A DUDH, proclamada em 1948 pela ONU, veio proclamar a ascensão dos direitos humanos e a respetiva proteção jurídica nas diversas Nações. Esta declaração veio atribuir um caráter universal pelo respeito dos direitos e liberdades fundamentais do homem num momento ainda conturbado, uma vez que ainda estavam bem patentes os resquícios da Segunda Guerra Mundial, bem como se constituiu como a "base e a inspiração para tratados e documentos jurídicos que se seguiriam no capítulo dos direitos humanos[745]".[746]

A CEDH da autoria do Conselho da Europa vigora na ordem internacional desde 1953 e em Portugal desde 1978, na qual estão patentes vários preceitos e protocolos que visam evidenciar a proteção dos direitos e liberdades fundamentais do homem a nível europeu[747]. O respeito pelos direitos humanos é controlado judicialmente pelo Tribunal Europeu dos Direitos do Homem, previsto no título II da CEDH.

---

[745] Destacamos os artigos 5.º e 9.º que determinam, respetivamente, que "ninguém será submetido a tortura nem a tratamentos cruéis, desumanos ou degradantes" e que "ninguém pode ser arbitrariamente preso, detido ou exilado". O art. 8.º prevê o "recurso efetivo contra os actos que violem os direitos fundamentais reconhecidos pela Constituição ou pela lei", a que qualquer cidadão tem direito.

[746] ALVES, David – **Uso excessivo da força. Questões jurídicas, técnico-policiais e sociais.** Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna, 2016. Dissertação de Mestrado. p. 24.

[747] O art.º 2.º protege o direito à vida e estatui que o artigo não é violado quando a morte resulte de recurso à força, tornado absolutamente necessário: para assegurar a defesa de qualquer pessoa contra uma violência ilegal; para efectuar uma detenção legal ou para impedir a evasão de uma pessoa detida legalmente; [e] para reprimir, em conformidade com a lei, uma revolta ou uma insurreição. Esta ressalva aplica-se, logicamente e por maioria de razão, às ofensas à integridade física que não resultem em morte. Paralelamente à DUDH, a CEDH determina que "ninguém pode ser submetido a torturas, nem a penas ou tratamentos desumanos ou degradantes" e reconhece o direito ao recurso efetivo no caso de violações a direitos protegidos na Convenção, ainda que sejam cometidas "por pessoas que atuem no exercício das suas funções oficiais." *Ibidem*.

Já em 1979 foi adotado pela Assembleia Geral das NU o código de conduta para os funcionários responsáveis pela aplicação da lei, através da Resolução n.º 34/169, de 17 de dezembro de 1979, o qual se destina preferencialmente a elementos policiais, considerando que este "permite regular a atividade policial ao elencar a importância dos direitos humanos a que os aplicadores da lei, pelas responsabilidades que lhes são impostas, devem especialmente atender"[748].

De igual modo, o Código de Conduta para os Funcionários Responsáveis pela Aplicação da Lei, reconhecido pela Assembleia Geral das NU, dispõe no seu art.º 3ºque "os Funcionários responsáveis pela aplicação da lei só podem empregar a força quando tal se afigure estritamente necessário e na medida exigida para o cumprimento do seu dever"[749].

Posteriormente, em 1990,foram aprovados pela Assembleia Geral das NU os Princípios Básicos sobre a Utilização da Força e de Armas de Fogo pelos Funcionários Responsáveis pela Aplicação da Lei, os quais genericamente defendem que "o recurso à força e à arma de fogo só são admitidos quando outros meios se revelam ineficazes ou incapazes de produzirem o resultado pretendido (Princípio 4)"[750].Nos casos em que os mesmos são utilizados legitimamente, "os responsáveis pela aplicação da lei deverão: exercer moderação no uso de tais recursos e agir na proporção da gravidade da infração e do objetivo legítimo a ser alcançado; minimizar danos e ferimentos, e respeitar e preservar a vida humana" (Princípio 5), bem como terá de ser obrigatoriamente comunicado superiormente o recurso ao uso da força (Princípio 6)[751].

Com efeito, poderemos concluir que ao nível internacional existem diversos normativos que regulam o uso da força pelas polícias portuguesas.

No que respeita à UE, os seus princípios basilares passam pela promoção da paz e por garantir a segurança dos seus cidadãos e do seu território, ao mesmo tempo que consi-

---

[748] O art.º 3.º estatui que "os funcionários responsáveis pela aplicação da lei só podem empregar a força quando estritamente necessária e na medida exigida para o cumprimento do seu dever". Segundo o art.º 5.º, nenhum funcionário responsável pela aplicação da lei pode infligir, instigar ou tolerar qualquer acto de tortura ou qualquer outro tratamento ou pena cruel, desumano ou degradante nem nenhum destes funcionários pode invocar ordens superiores ou circunstâncias excepcionais (…) como justificativa para torturas ou outros tratamentos ou penas cruéis, desumanos ou degradantes. *Ibidem*.

[749] ALVES – ***Op cit.*** p. 25.

[750] *Ibidem*.

[751] Em complemento, refira-se que o princípio 9 determina que "os responsáveis pela aplicação da lei não usarão armas de fogo contra pessoas, exceto em casos de legítima defesa própria ou de outrem contra ameaça iminente de morte ou ferimento grave; para impedir a perpetração de crime particularmente grave que envolva séria ameaça à vida; para efetuar a prisão de alguém que represente tal risco e resista à autoridade; ou para impedir a fuga de tal indivíduo, e isso apenas nos casos em que outros meios menos extremados revelem-se insuficientes para atingir tais objetivos. Em qualquer caso, o uso letal intencional de armas de fogo só poderá ser feito quando estritamente inevitável à proteção da vida." *Ibidem*.

deram que a segurança interna e externa estão cada vez mais interligadas, devido a que a sua "segurança interna depende da paz nas regiões para além das [suas] fronteiras"[752].

3.1.2. O Uso da Força em Portugal

O Estado[753] detém o monopólio do uso da força em Portugal, pelo que o seu papel na Segurança Interna (SI) se revela fundamental.

Com efeito, podemos afirmar que no emprego da força pública, apenas "ao Estado de Direito democrático pertence o monopólio de regulação do emprego da força, isto é, o monopólio estadual de definição das condições de emprego da força, a que corresponde também a posição dominante de emprego da força"[754].

Em complemento, refira-se que a "globalização aumentou a proximidade entre as pessoas, as organizações e os Estados, intensificando as relações e os processos de mudança, acarretando como consequência, novos fenómenos criminais, que pela sua complexidade, dimensão ou alcance, ultrapassam fronteiras, impondo a consciência da vulnerabilidade da segurança pessoal, face a fenómenos como o terrorismo, que, de longínquo, passou a ameaça presente e próxima no contexto Europeu, a que nenhum país está imune"[755].

Este paradigma mundial vem dificultar ainda mais uma delimitação do contexto do uso da força, seja ao nível nacional ou mundial.

Neste contexto, recordemos que, para que se possa falar da "existência de um Estado, é necessário a existência de um povo e de um território, mas é preciso acrescentar a esses dois elementos um poder[756] político, ou seja, é preciso que exista um poder capaz de impor ao grupo regras de conduta social e dotado de autoridade para se fazer obedecer"[757].

---

[752] UNIÃO EUROPEIA – **Visão partilhada, ação comum: uma Europa mais forte. Estratégia global para a política externa e de segurança da UE.** 2016. p. 5.

[753] "O Estado é a estrutura juridicamente personalizada, que num dado território exerce um poder político soberano, em nome de uma comunidade de cidadãos que ao mesmo se vincula." Cfr. AAVV, **Enciclopédia de Direito e Segurança** (coord. de Jorge Bacelar Gouveia e Sofia Santos). Coimbra: Almedina, 2015.

[754] CLEMENTE, Pedro – Polícia e Segurança – breves notas. In **Lusíada. Política Internacional e Segurança.** N.º 4, 2010. p. 149.

[755] NOGUEIRA, Pedro – **Modelos híbridos de Segurança, o desafio da dimensão Público-Privada.** Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2016.

[756] O Poder não é uma coisa, é uma relação, porque não há poder senão na medida em que outros são dominados ou influenciados. Pode haver uma colectividade fixa num território e não constituir um Estado; o Estado, só nasce quando essa colectividade for dotada de um aparelho de poder capaz de se fazer obedecer e impor as normas de comportamento a todos os membros do grupo. Cfr. MOREIRA, Adriano – **Ciência Política**. Coimbra: Almedina, 1997. p. 48.

[757] SANTOS, Aristofanes – **O uso da força no exercício da função policial (Alguns aspectos legais).** Lisboa: Instituto Superior de Ciências Policiais e de Segurança Interna, 2002. Tese de Licenciatura. p. 48.

O Estado é igualmente o responsável pela promoção da "defesa dos demais direitos pessoais, culturais, sociais e económicos através da ação das forças de segurança e demais instituições e entidades englobantes no conceito de polícia"[758].

Deste modo, o papel do Estado nesta matéria "pode ser definido como um dos recursos, que este tem ao seu dispor, para que de forma preventiva ou repressiva, salvaguardar eventuais comportamentos oriundos de terceiros, que coloquem em causa direitos fundamentais dos cidadãos; e num sentido mais amplo, a segurança do próprio Estado"[759].

Com efeito, a temática da SI assenta na premissa de que o Estado é a "instituição que detém o monopólio da violência legítima na sociedade"[760].

A SI em Portugal é garantida através das respetivas FS: Guarda Nacional Republicana e Polícia de Segurança Pública.

Relativamente ao uso da força pelas FS em Portugal, o mesmo é enquadrado juridicamente ao nível nacional e internacional, tal como já vimos.

No caso nacional, esta problemática encontra previsão legal na CRP, enquanto texto fundamental da nossa democracia, onde se encontram "tipificados todos os direitos fundamentais dos cidadãos e prevista a excecional possibilidade de restrições"[761].

De igual modo, na CRP vem igualmente prevista a Polícia na orgânica da AP, que lhe atribui as respetivas funções e que impõe limites à sua atividade[762].

Neste contexto, e de acordo com o texto constitucional, falarmos em "violência legítima" leva-nos a concluir que "este tipo de comportamento só é admitido ao Estado, e única e exclusivamente como forma de repelir qualquer ameaça que atente contra a sua segurança, que ao ser posta em causa, produzirá obviamente efeitos negativos para a população, pondo em questão os tão aclamados e defendidos direitos, liberdades e garantias que esse mesmo Estado promove para a sua população"[763].

A atual CRP, nos seus artigos 17.º e 18.º, vem concretizar o conceito de "violência legítima" e, de igual modo, tipificar a forma como este tipo de violência pode ser exercida, nos termos do seu art.º 272º, onde se encontram definidas as atribuições de Polícia. Estas funções são "exercidas pelos mais variados órgãos do Estado, para além da competência

---

[758] VALENTE, Manual – **Teoria Geral do Direito Policial**. 3ª Ed. Coimbra: Almedina, 2012. p. 110.
[759] FERREIRA – ***Op cit.*** p. 27.
[760] *Ibidem*.
[761] ALVES – ***Op cit.*** p. 26.
[762] "Há ainda um vasto leque de documentos jurídicos, relativos a diversas matérias, que dispõem de preceitos sobre a proteção dos direitos humanos e o recurso policial ao uso da força. Todavia, todos eles estão forçosamente em sintonia com a lei constitucional, a lei suprema do Estado de direito." *Ibidem*.
[763] *Ibidem*.

para manter a ordem pública, no caso de estarem em causa esses mesmos direitos, liberdades e garantias, no que concerne a aspetos relacionados com a SI"[764].

O art.º 266° da CRP diz respeito aos princípios basilares que regem a Administração Pública, os quais definem que esta "visa a prossecução do interesse público, no respeito pelos direitos e interesses legalmente protegidos dos cidadãos" (n.º 1); e que "os órgãos e agentes administrativos estão subordinados à Constituição e à lei e devem atuar, no exercício das suas funções, com respeito pelos princípios da igualdade, da proporcionalidade, da justiça, da imparcialidade e da boa fé" (n.º 2).

Já no seu art.º 272º, a CRP destina à Policia a função de "defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos" (n.º 1), assumindo-se estes direitos como o cerne da atual policial. Deste modo, a "prevenção dos crimes, incluindo a dos crimes contra a segurança do Estado, só pode fazer-se com observância das regras gerais sobre polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos" (n.º 3), considerando o direito à segurança e o direito à liberdade. Assim, o uso da força é limitado aos princípios da subsidiariedade, necessidade e proporcionalidade.

No seguimento do texto constitucional, a Lei de Segurança Interna[765] (LSI) consagra no seu art.º 35.º uma referência expressa às FA quando define que "as FA colaboram em matéria de segurança interna nos termos da Constituição e da Lei, competindo ao Secretário-Geral do Sistema de Segurança Interna (SSI) e ao Chefe do Estado-Maior-General das FA assegurarem entre si a articulação operacional".

A referida colaboração, que ocorrerá nos termos do art.º 35.º da LSI deverá faz-se nos termos do disposto nos números 6 e 7 do art.º 275.º da CRP[766].

Em complemento, sublinhe-se que as FA podem ser igualmente empregues em casos de estado de sítio e de estado de emergência, de acordo com o art.º 19.º da CRP.

---

[764] "Em suma o papel do Estado em matéria de SI consiste na defesa de todos os órgãos que o constituem, e sociedade civil, a fim de garantir fatores como a segurança de pessoas e bens, através da promoção e efetivação dessa mesma segurança e tranquilidade pública e ordem democrática, contra qualquer tipo de ameaça que possa colocar em causa algum destes fatores, sendo que para o efeito, o Estado detém o direito exclusivo de através dos organismos designados para o efeito, o recurso a medidas e formas de atuação de cariz repressivo, e que se encontram previstos e condicionados em diversos diplomas legais e sempre em consonância com a CRP." FERREIRA, Renato – Globalização e Segurança. Um mundo em mudança. In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 8 Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2015. p. 27-28.

[765] Lei N.º 53/2008. **Diário da República I Série.** N.º 167 (29-08-2008). p. 6135-6141.

[766] "As FA podem ser incumbidas, nos termos da lei, de colaborar em missões de proteção civil, em tarefas relacionadas com a satisfação de necessidades básicas e a melhoria da qualidade de vida das populações, e em ações de cooperação técnico-militar no âmbito da política nacional de cooperação."

Deste modo, podemos então constatar a necessidade de encontrar uma estratégia de Segurança Interna para Portugal.

Tal desiderato, encontra suporte na premissa atualmente em vigor de que se a ameaça for externa, a SI apoia a Defesa Nacional. Já nas "situações em que a ameaça é interna, o esforço predominante para a segurança nacional compete à Segurança Interna, devendo as FSS serem apoiadas supletivamente pelas FA, sempre que necessário"[767].

Com efeito, afigura-se como essencial um Conceito Estratégico de SI no sentido de uma possível "redefinição da arquitetura do Sistema de Segurança Nacional, seguindo uma lógica de complementaridade multi sistema que englobe, nomeadamente, a segurança militar, SI, informações, justiça e proteção civil, enquanto origem de uma "futura e necessária" Estratégia Nacional de SI que traduza as necessidades, a experiência e a evolução dos SSI dos vários Estados que integram o espaço de liberdade, segurança e justiça da UE"[768].

De igual modo, refira-se que "qualquer Estratégia de Segurança Interna de âmbito nacional deve aglutinar conteúdos europeus e nacionais de outras estratégias. Assim, deve ser considerada a sua concordância e coerência com as seguintes estratégias específicas: estratégia de segurança interna da UE[769]; (…) Estratégia da UE para a cibersegurança; estratégia da UE para a luta contra a radicalização e o recrutamento do terrorismo"[770].

Por outro lado, consideramos que a SI devera ocorrer no espaço terrestre, no mar territorial, no espaço aéreo e ciberespaço. Deste modo, e tendo em consideração um quadro complexo de ameaças e as "competências em termos de missões a executar no âmbito da atividade de segurança interna, verifica-se que são necessárias capacidades próprias, tais como: na utilização do espaço aéreo; no âmbito da cibersegurança; e ao nível do comando e controlo da atividade operacional"[771].

No que respeita à cibersegurança constatamos que a "partilha da informação e a cooperação constituem elementos decisivos na prevenção e no "combate"ao diferente espetro das ciberameaças. Também neste âmbito não existe presentemente uma estratégia nacional

---

[767] LOURENÇO et al. – **Segurança Horizonte 2025. Um Conceito Estratégico de Segurança Interna.** Lisboa: Edições Colibri, 2015. p. 18.
[768] LOURENÇO et al. – ***Op cit.*** p. 23, 24, 87.
[769] As prioridades são: desmantelar as redes internacionais de criminalidade; prevenir o terrorismo e responder à radicalização e ao recrutamento; reforçar os níveis de segurança para os cidadãos e as empresas no ciberespaço; reforçar a segurança através da gestão de fronteiras; reforçar a capacidade de resistência da Europa às crises e catástrofes.
[770] LOURENÇO et al. – ***Op cit.*** p. 50.
[771] LOURENÇO et al. – ***Op cit.*** p. 59.

única, coexistindo, em contrapartida, iniciativas avulsas com a virtuosa finalidade de fazer face a este problema de segurança"[772].

Em complemento, registe-se que o "SSI deve igualmente considerar as linhas orientadoras da UE em vetores cruciais, como seja a cibersegurança[773], pugnar por uma direção política mais coordenada e pelo princípio da coordenação e cooperação entre FSS"[774].

Voltando à problemática do uso da força, constatamos que este se constitui como um "instrumento indispensável ao Estado, e este é, por tal razão, o detentor do monopólio da violência física legítima"[775].

O Estado, para Weber[776], representa uma relação de dominação e "só pode existir (…) sob condição de que os homens dominados se submetem à autoridade continuamente reivindicada pelos dominadores", isto é, no designado contrato social são os cidadãos que abdicam do "recurso próprio à violência como forma de resolver conflitos, consignando esta prerrogativa no Estado".[777]

Neste sentido, o Estado concretiza-se como um sistema social com "o monopólio ou a exclusividade da satisfação de necessidades coletivas"[778] que tem ao seu dispor vários recursos, no qual se inclui o recurso à força coativa, ou seja, "o Estado recorre a determinados meios para se impor como regulador social, sendo que um deles é a violência, o seu instrumento de domínio específico"[779].

Atualmente constatamos que a "violência legítima constitui um atributo da autoridade do Estado, que se arroga do seu monopólio"[780], ou seja, o seu uso está vedado terceiros, o que quer dizer que "mais ninguém pode recorrer a este meio de forma legítima[781]. O uso

---

[772] O Ministério da Defesa Nacional formulou as medidas correspondentes com a respetiva estratégia particular, a Autoridade Nacional de Segurança obedece ao seu racional próprio e as FSS apresentam medidas que importa igualmente alinhar pelos objetivos nacionais. Também neste domínio, quer o impulso nacional seja externo ou interno, a finalidade deverá ser única. LOURENÇO et al. – ***Op cit.*** p. 61-62.

[773] A UE definiu em 7 de fevereiro de 2013 uma Estratégia de Cibersegurança Europeia, que compreende 6 eixos de atuação: combate ao crime; normalização e certificação; proteção de infraestruturas críticas; formação e consciencialização; alerta e resposta a incidentes; e investigação e desenvolvimento. Consultar a Comunicação Conjunta ao PE, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a estratégia da UE para a Cibersegurança, Bruxelas, 7.2.2013 – JOIN (2013).

[774] LOURENÇO et al. – ***Op cit.*** p. 68.

[775] ALVES – ***Op cit.*** p. iv.

[776] WEBER, M. – **Ciência e Política duas vocações**. 14º Ed. Berlim: Dunker & Hunblot, 2007. p. 57.

[777] ALVES – ***Op cit.*** p. 5.

[778] OTERO, Paulo – **O Poder de Substituição em Direito Administrativo: Enquadramento Dogmático-Constitucional.** Vol. I e II. Lisboa: Lex, 1995. p. 48.

[779] ALVES – ***Op cit.*** p. 5.

[780] MATIAS, A. – **A Violência no Mundo Moderno**. Lisboa: Livraria Bertrand, 1978. p. 12.

[781] "Ao concentrar no Estado e nas suas instituições de controlo social o monopólio do uso legítimo dos meios de violência, a ordem jurídica "expropria" dos indivíduos o recurso à violência como meio de alcançar os fins, e realiza um elemento central da noção de cidadania, isto é, cabe apenas ao Estado, pelas instituições que dirige, a proteção contra a ameaça criminosa." MILITÃO – ***Op cit.*** p. 297.

da violência, por ter sérias repercussões na esfera jurídica das pessoas, [pelo que] só pode ser justificado no quadro do dever estadual de proteger os direitos humanos"[782].

Deste modo, "o uso legítimo da força faz parte do quadro de ações possíveis do Estado e constitui seu monopólio específico, baseado numa relação de legitimidade"[783]. Assim, a polícia fica encarregue de concretizar a ligação ao poder legalmente instituído.[784]

Neste paradigma, a força coativa do Estado português, divide-se em duas partes: FA e FS[785]. As FS são constituídas pela Guarda Nacional Republicana e pela Polícia de Segurança Pública, as quais respondem pela utilização da força coativa no plano interno, a fim de assegurar o respeito pela Lei[786].

Todavia, esta necessidade do uso da força moderada e do respeito pelo princípio da legalidade baseia-se no respeito pelas Leis que, de "acordo com a soberania de cada Estado se afigura imprescindível a sua manutenção, ou seja, o uso da força não significa correntemente uma expressão de arbitrariedade e dominação do povo, mas tão só o exercício do poder de autoridade na consecução de um interesse público específico"[787]. Neste sentido, "os funcionários responsáveis pela aplicação da lei só podem empregar a força quando tal se afigure estritamente necessário e na medida exigida para o cumprimento do seu dever"[788], ou seja, a aplicação da força só se deve verificar quando tal se afigure estritamente necessário e sempre de forma proporcional[789] ao cumprimento do seu dever.[790]

Daqui resulta "a natureza residual e subsidiária do uso da força policial, ao mesmo tempo que se consignam os princípios da necessidade e da proporcionalidade, sempre na perspetiva do exercício de um dever e nunca no exercício de um direito"[791].

---

[782] ALVES – ***Op cit.*** p. 6.
[783] CLEMENTE, Pedro – **Da Polícia de Ordem Pública.** Lisboa: Governo Civil, 1998. Dissertação de Mestrado. p. 47.
[784] SANTOS – ***Op cit.***2002.p. 49.
[785] As FA vinculam-se mais à sustentação dos valores mais consensuais, integridade nacional e defesa militar do país, enquanto as FS se ocupam mais "dos valores prosaicos da vida quotidiana (ordem pública preventiva e repressiva)". Cfr. CLEMENTE – ***Op cit.*** 1998. p. 47.
[786] Tendo em conta que "não existe sociedade sem Instituição e não há Instituições sem poder e sem autoridade que faça respeitar esse poder, se necessário, pela força", pensamos que se justifica a necessidade do uso da força coactiva em casos extremos, mas tendo sempre em atenção os limites dessa atuação. CLEMENTE – ***Op cit.*** p. 43.
[787] CLEMENTE – ***Op cit.*** p. 50. e SANTOS – ***Op cit.***2002.p. 50.
[788] Cfr. Art.º 3º do Código de Conduta para os Funcionários Responsáveis pela Aplicação da Lei.
[789] Importa realçar que, do ponto de vista da legislação Portuguesa, o uso da força é restringido ao princípio da proporcionalidade, pelo que este princípio deve ser estritamente respeitado, ou seja, o emprego da força por parte dos funcionários responsáveis pela aplicação da lei não deve ser feito em desproporção com o legitimo objectivo a atingir, sob pena de os seus agentes incorrerem em responsabilidade criminal.
[790] SANTOS – ***Op cit.*** 2002. p. 51.
[791] "Na verdade, o emprego da força só se deve verificar em casos extremos ou excecionais, não obstante o facto de a própria lei admitir a utilização da força nos casos em que esta seja necessária tendo sempre em conta a razoabilidade da situação, de acordo as circunstâncias, para a prevenção de um crime ou para deter ou

Neste paradigma, verifica-se que a "especificidade da execução administrativa face à execução processual-civil reside no facto de o próprio Estado criar o título executivo, através da prática de um ato administrativo que contém uma "ordem", de cumprimento obrigatório, podendo ser imposta, se necessário, coativamente, isto é, pela força"[792].

A multiplicidade dos desafios ditos clássicos a que a SI tem geralmente de fazer face inclui "ameaças como a desordem civil, atos de violência em larga escala, ou mesmo invasões ou insurgências que ponham em cheque a soberania e/ou o monopólio que cada Estado detém sobre o uso da força no seu território e sobre a sua população"[793].

Inerente ao uso da força surge a legítima defesa[794], na qual "os agentes de autoridade estão legitimados ao uso da força desde que haja justificação plausível[795]. A legítima defesa exige que se verifique uma agressão atual e ilícita aos interesses juridicamente protegidos de uma pessoa que se defende ou de terceiros, com o intuito desta factualidade permitir a prática de um evento necessário a repelir uma agressão com vista a paralisar o agressor.

Porém, será essencial "analisar os meios a empregar, ou seja, tem de haver proporcionalidade nos meios a utilizar, não sendo admissíveis excessos, sob o risco de cair em excesso de legítima defesa"[796]. Neste particular, refira-se que a "avaliação do uso da força está dependente de um conjunto de circunstâncias concretas que definem cada situação"[797].

Ao mesmo tempo, nos casos de alteração de ordem pública ou nas "situações de particular gravidade e atentatórias da segurança de pessoas ou bens, o Estado poderá manifestar-se através de uma ação policial repressiva que usa a força como meio"[798], no sentido da promoção dos direitos humanos e da reposição da ordem pública, situações que podem, por vezes, exigir uma coerção de natureza física.

Recentemente, surgiu um novo tipo de policiamento guiado pelas informações, o qual se consubstancia como uma alternativa ao uso da força.

---

ajudar à detenção legal de delinquentes ou de suspeitos." Cfr. MAXIMIANO, António – Qualidade de Acção policial. In **Seminário sobre parâmetros jurídicos da actuação Policial**. Lisboa: IGAI, 1996. p. 16.

[792] "O recurso contencioso não visa, geralmente, a obtenção de um título executivo, mas apenas o controlo jurídico do "título executivo" criado pela ação ou omissão da Administração e/ ou o controlo da sua execução." SOUSA, António – **A Polícia no Estado de Direito.** Lisboa: Editora Saraiva, 2009. p. 287-288.

[793] ELIAS, Luís; GUEDES, Armando – **Controlos Remotos: Dimensões Externas da Segurança Interna em Portugal.** Lisboa: Almedina, 2010. ISBN 9724043576. p. 425.

[794] Cfr. Art.º 32.º do Código Penal.

[795] Cfr. Código de Conduta para os Funcionários Responsáveis pela Aplicação da Lei, tendo como anexo os "Princípios Básicos Sobre a Utilização da Força e das Armas de Fogo pelos Responsáveis pela Aplicação da Lei", bem como as leis orgânicas e diplomas complementares das diferentes Forças de Segurança, e, genericamente, nos preceitos legais sobre Legitima Defesa, enquanto causa de exclusão da ilicitude.

[796] Cfr. Art.º 33.º do Código Penal. e SANTOS – ***Op cit.*** 2002. p. 9.

[797] "O uso excessivo da força não é, seguramente, um conceito mensurável pela quantidade de força empregue já que, em determinados casos, até o uso da força letal pode ser legítimo."ALVES – ***Op cit.*** p. 7.

[798] ALVES – ***Op cit.*** p. 7.

Este modelo de policiamento, internacionalmente designado de *intelligence-led policing*, é guiado pelas informações e "emerge como o modelo de ação policial em que o produto informacional dirige o esforço de patrulhamento uniformizado, para dissuadir a prática de incivilidades, muitas delas uma expressão adolescente da contra-cultura urbana"[799]. Este método aplicado pelo "policiamento guiado pelas informações alicerça-se: na pesquisa de notícias, através de meios humanos, incluindo a vigilância de suspeitos; no recurso à tecnologia, incluindo a videovigilância da via pública; na exploração de fontes de informação, habitualmente abertas, incluindo a imprensa local"[800].

3.2. Proibição Internacional do Uso da Força

O Direito Internacional estabelece a "base normativa orientadora do recurso ao uso da força de modo legítimo por parte dos Estados", uma vez que "o uso da força nas relações internacionais não pode ser efetuado de forma arbitrária".[801]

Nesta perspetiva, a "CNU detém um valor substantivo inalienável pelo facto de ter permitido a cristalização do Direito Internacional"[802], não obstante lhe sejam ainda reconhecidas algumas insuficiências normativas, considerando que "o sistema onusiano não tem conseguido impedir o uso da força para além dos parâmetros jurídico-normativos estabelecidos"[803].

Em complemento, registe-se que, de acordo com a Convenção de Viena sobre o Direito dos Tratados, assinada em 23 de Maio de 1969, e tendo por base os princípios de direito internacional consignados na CNU, a proibição da ameaça ou do emprego da força se constituem como direitos universais e efetivos dos direitos do homem e das liberdades fundamentais para todos.

De igual modo, a temática do uso da força no DIP continua a ser um tema central à segurança internacional, porquanto "o princípio geral da proibição do seu emprego integra hoje um dos pilares fundamentais da ordem internacional construída depois da II Guerra-

[799] CLEMENTE, Pedro – Informações e Segurança Pública In MOREIRA, Adriano; RAMALHO, Pinto (coord.) – **Estratégia.** Vol. XIX. Lisboa: Instituto Português da Conjuntura Estratégica, 2010. p. 419.
[800] *Ibidem*.
[801] SANTOS – ***Op cit.*** 2012. p. 533-534.
[802] *Ibidem*.
[803] "As novas ameaças bem como as divergentes interpretações da Carta, quer entre os EM quer na doutrina jusinternacionalista, têm dificultado a sua aplicação eficaz e a produção de segurança jurídica." SANTOS – ***Op cit.*** 2012. p. 534.

Mundial"[804], motivo pelo qual a CNU vem definir no seu art.º 1º, n.º 1, como objetivo fundamental das NU, a manutenção da paz e segurança internacionais.

Todavia, o art.º 2º, n.º 4, desta Carta veio introduzir um princípio geral de proibição do uso da força, o qual se reveste de particular importância. Esta norma vem deste modo não só proibir o uso da força, como também a "simples ameaça deste recurso contra a integridade territorial ou a independência política de um Estado, quer seja de qualquer outro modo incompatível com os objetivos das NU"[805], pelo que não poderemos separar este princípio geral do dever de resolução pacífica de conflitos internacionais por parte dos EM, de acordo com os termos do art.º 2º, n.º 3, e do Capítulo VI da Carta.

Por outro lado, "a condenação da guerra e do uso da força não significa uma exclusão categórica dessa possibilidade"[806], uma vez que a CNU prevê exceções ao princípio estabelecido no art.º 2º, n.º 4, as quais "incluem uma série de premissas que constituem uma orientação normativa para o recurso ao uso da força nas relações internacionais"[807].

A legítima defesa, nos termos do art.º 51.º da CNU, constitui-se como a primeira exceção à regra da proibição da ameaça ou do uso da força, qualquer que seja a modalidade do uso da força no exercício de legítima defesa individual ou coletiva[808].

Desta forma, a legítima defesa vem possibilitar que se verifique uma exceção à "proibição do uso da força nas relações internacionais, autorizando que os Estados, diante de um ataque armado, recorram à violência, omitindo-se no que diz respeito à possibilidade de se alegar legítima defesa preemptiva, diante da iminência de um ataque armado e não de um ataque efetivo"[809].

Neste sentido, a CNU vem preconizar no seu art.º 42.º a admissibilidade de medidas militares, definindo que se "o CS considerar que as medidas previstas no art.º 41.º seriam ou demonstraram ser inadequadas, poderá levar a efeito, por meio de forças aéreas, navais ou terrestres, a ação que julgar necessária para manter ou restabelecer a paz e a segurança

---

[804] "O uso da força nunca deixou de estar presente como tópico fundamental das relações internacionais ao longo dos tempos no plano da reflexão ético-filosófica, sempre concentrando polémicas importantes acerca da legitimidade e dos limites da guerra como direito dos Estados." GOUVEIA, Jorge – O uso da força no DIP. In **Revista Brasileira de Estudos Políticos.** N.º 107. Belo Horizonte: 2013. (julho/dezembro). p. 1.
[805] SANTOS – ***Op cit.*** 2012. p. 537.
[806] *Ibidem*.
[807] *Ibidem*.
[808] A legítima defesa será abordada mais adiante num subcapítulo próprio.
[809] "No entanto, o art.º 51.º da CNU possibilita que os Estados, individualmente considerados, recorram ao uso da força, de forma lícita, em resposta a um ataque armado, sendo importante perceber que "o uso da força somente é lícito, no âmbito internacional, para fins de manutenção ou restabelecimento da paz e segurança internacionais." ROSA, Patrícia; SILVA, Carla – **O uso da força em direito internacional – legítima defesa preemptiva.** Universidade de Itaúna, [s.d.]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.publicadireito.com.br/art.ºs/?cod=a08c938c1e7c76d8. p. 1 e 2.

internacionais. Tal ação poderá compreender demonstrações, bloqueios e outras operações, por parte das forças aéreas, navais ou terrestres dos membros das Nações Unidas".

Assim, o CS poderá optar pela decisão de impor sanções coativas militares, as quais poderão ser concretizadas através de demonstrações, bloqueios e outro tipo de operações. Contudo, a adoção de medidas previstas no art.º 42.º terá de ser conjugada com os artigos previstos no Capítulo VII[810], "segundo o qual o recurso a sanções coativas militares é considerado uma medida de *ultima ratio*"[811]. De acordo com este Capítulo, o CS alcança uma vasta "capacidade de ação com vista à concretização da sua responsabilidade primária de manutenção da paz e segurança internacionais consagrada no art.º 24º, n.º 1"[812].

As restantes exceções que são admissíveis à proibição geral do uso da força são as consignadas nos artigos 107.º e 53.º, n.º 1.

O art.º 107.º veio preconizar a designada cláusula sobre Estados inimigos, a qual inclui uma "reserva que é válida para os antigos adversários na Segunda Guerra Mundial, designadamente, o Japão, a Alemanha e a Itália"[813]. Este artigo define que "a CNU não deve invalidar ou impedir qualquer ação que na sequência da segunda guerra mundial seja levada a efeito ou autorizada contra estes Estados"[814].

Já o art.º 53º, n.º 1, presente no Capítulo VIII da CNU, "que regula as relações entre as NU e as organizações e acordos regionais, prevê a possibilidade de recurso à força por parte destas, porém sob condição de existir uma autorização prévia do CS"[815]. Todavia, realce-se que este artigo só é aplicável quando as partes não conseguirem alcançar uma solução pacífica das controvérsias, nos termos do art.º 52º.

---

[810] "Ao constituir o núcleo do sistema de segurança coletiva das NU, o Capítulo VII assume um papel central na implementação do seu objetivo primordial estipulado no art. 1º, n.º 1 da Carta que prevê a possibilidade de medidas coletivas com o propósito "de prevenir e afastar ameaças à paz e reprimir os atos de agressão, ou outra qualquer rutura da paz e chegar, por meios pacíficos, e em conformidade com os princípios da justiça e do Direito Internacional, a um ajustamento ou solução das controvérsias ou situações internacionais que possam levar a uma perturbação da paz." SANTOS – ***Op cit.*** 2012. p. 539.

[811] "A aplicação das medidas previstas pressupõe a determinação da existência de uma ameaça à paz, rutura da paz ou ato de agressão nos termos do art. 39º e que as medidas provisórias e as sanções coativas não militares de acordo com os artigos 40º e 41º, respetivamente, não pudessem ser ou não se tenham revelado eficazes. À semelhança do art. 51º, este artigo encontra-se limitado juridicamente pelo princípio da proporcionalidade, que se pode inferir igualmente pela referência ao art. 41º." *Ibidem*.

[812] Este órgão garante o respeito da norma imperativa com base neste capítulo e através da promoção, num primeiro momento, de uma solução pacífica dos conflitos como preceituado no n.º 3 do art. 2º e no Capítulo VI da Carta. *Ibidem*.

[813] SANTOS – ***Op cit.*** 2012. p. 540.

[814] *Ibidem*.

[815] "De salientar que o art.º 53.º faz referência ao art.º 107.º ao determinar que, a título de exceção, uma ação coercitiva pode ser levada a cabo sem a autorização do Conselho contra um "Estado inimigo", precisando no n.º 2 esta noção." SANTOS – ***Op cit.*** 2012. p. 541.

Face ao exposto, concluímos que estas exceções devem ser vistas numa perspetiva diferente daquelas que foram anteriormente referidas. Tal, assenta na questão do art.º 107º se poder considerar uma disposição obsoleta e, logo, sem aplicabilidade, e o recurso à força por parte das organizações regionais significar uma descentralização do uso da força, ou seja, uma transferência da responsabilidade jurídica dos EM prevista no art.º 42.º.[816]

Com efeito, constatamos que o estabelecimento de uma proibição genérica do uso da força e inerentes exceções não se concretizou "numa completa ausência do recurso ilegítimo ao uso da força"[817], uma vez que tal seria um pouco utópico, considerando "a multidimensionalidade e mutabilidade das relações internacionais"[818]. Como tal, "não se pode permitir um desrespeito recorrente do Direito Internacional. Ao se tratar de uma norma de caráter imperativo e inderrogável, este facto assume uma maior relevância."[819]

Em complemento, não poderemos olvidar que o sistema onusiano foi inicialmente projetado "com base no modelo clássico de conflitos, de cariz interestadual, [pelo que] o sistema tem tentado adaptar-se às novas formas de conflito e cenários de ameaça à paz e segurança internacionais"[820].

Deste modo, o seu principal problema reside no facto da necessidade de evolução e adaptação "de modo a fazer face às ameaças à segurança nas relações internacionais, encontrando-se a sua interpretação e extensão no centro de uma divisão profunda entre EM e na doutrina jusinternacionalista", situação que ainda é agravada pelo motivo destas normas serem consideradas de "caráter vago e impreciso".[821]

Em complemento, importa ainda acrescentar que "a formulação ambígua do art.º 2.º, n.º 4, dificulta a determinação do seu conteúdo e alcance e gera incerteza relativamente ao

[816] *Ibidem*.
[817] *Ibidem*.
[818] *Ibidem*.
[819] *Ibidem*.
[820] Os conflitos intraestaduais, que têm sido o fenómeno dominante desde 1945, e as armas de destruição maciça e o novo terrorismo internacional representam ameaças que a Carta, como documento "pré-atómico", não poderia contemplar aquando da sua redação. Neste sentido, a Carta é considerada uma *living constitution*; a interpretação dinâmica das suas normas tem permitido uma "elasticidade" do sistema. A proteção dos direitos humanos constituiu o ponto de partida para uma relativização da proibição do uso da força em prol de outros valores fundamentais no Direito Internacional. SANTOS – ***Op cit.*** 2012. p. 542.
[821] "Se por um lado, esta ambiguidade possibilita uma maior flexibilidade do sistema para fazer face a desafios imprevisíveis e, consequentemente, uma evolução do próprio Direito Internacional, por outro lado, dificulta, (…) o alcance de um consenso entre os membros permanentes do CS – ao permitir uma interpretação unilateral de acordo com os seus interesses nacionais – e a uniformidade da aplicação do direito." *Ibidem*.

seu teor"[822], motivo pelo qual este artigo não deverá ser interpretado isoladamente, mas em conjugação com os artigos 39.º, 51.º e 53.º da Carta.

Por sua vez, o art.º 39.º do Capítulo VII da CNU vem dificultar a interpretação do alcance do mesmo, uma vez que a designação de "ameaça à paz", "rutura da paz" e "ato de agressão" não se "encontram definidas nem na Carta nem nas decisões dos órgãos das NU de forma indubitável, requerendo sempre uma interpretação caso a caso por parte do CS"[823]. A título de exemplo, refiram-se as resoluções 1368 e 1373, de 2001, nas quais consta "o terrorismo internacional como uma ameaça à paz nos termos do art.º 39.º"[824] da CNU, não obstante subsistira possibilidade de diferentes interpretações.

Por outro lado, existem ainda outros fatores delimitadores do paradigma onusiano que se encontram associados às especificidades do Direito Internacional: "a ausência de um legislador internacional, de uma jurisdição obrigatória e de uma instância de controlo, semelhante ao papel das forças policiais como se verifica no Direito Interno"[825].

Com efeito, neste momento poderemos sintetizar as seguintes ideias:

- As exceções ao princípio geral da proibição do uso da força são as seguintes: a legítima defesa, as sanções coativas militares ao abrigo do capítulo VII, as medidas adotadas por organizações regionais e as medidas adotadas contra anteriores Estados inimigos.
- A legítima defesa, direito consubstanciado no art.º 51.º da CNU, pressupõe a existência de um ataque armado contra um determinado Estado. Nestas circunstâncias, poderá existir

---

[822] "Estes artigos contêm conceitos, que apesar de estarem interligados, têm um significado muito díspar. Note-se que, as noções de ameaça ao uso da força, "ameaça à paz", "ataque armado" não se encontram definidas na Carta nem clarificadas na doutrina e na prática estadual de forma inequívoca. Em parte, por esta mesma razão, a tentativa de uma interpretação extensiva e uniforme da proibição do uso da força face a conflitos intraestaduais ou formas indiretas de uso da força tem enfrentado alguma resistência na prática estadual." SANTOS – ***Op cit.*** 2012. p. 543.

[823] Conceito de ameaça à paz: "Embora este conceito tenha sido deixado intencionalmente impreciso de forma a possibilitar uma ampla margem de apreciação, a sua clarificação assume uma grande relevância. Relembre-se que só após a determinação pelo Conselho de uma ameaça à paz, é que este pode determinar medidas provisórias e sanções coativas não militares ou militares para o restabelecimento da paz e segurança internacionais." SANTOS – ***Op cit.*** 2012. p. 548.

[824] SANTOS – ***Op cit.*** 2012. p. 549.

[825] "A inexistência de um mecanismo que assegure uma aplicação efetiva, constante e uniforme das normas jurídico-internacionais, sobretudo das normas *ius cogens* e *erga omnes* origina críticas, por vezes mais incisivas, relativamente à influência e autoridade do Direito Internacional. Contudo, o paradigma onusiano é perfetível." De igual modo, o "significado do papel do Conselho neste contexto não pode ser ignorado. Embora o CS não seja uma fonte de Direito Internacional, as suas decisões fazem evoluir este ramo do direito e o seu contributo seria mais significativo se se verificasse uma reinterpretação do *ius ad bellum* consagrado na Carta, uma introdução de critérios de legitimidade para o uso da força e da responsabilidade de proteger, reduzindo-se, portanto, a dependência do Direito Internacional de decisões políticas. O Conselho poderia, assim, contribuir para a implementação das obrigações *erga omnes*, para a determinação, em certa medida, do alcance e das consequências jurídicas desta conceção para a resolução do conflito normativo entre a soberania e integridade territorial de um Estado e o uso da força coletiva. Este consenso mais amplo sobre o uso da força permitiria a eliminação de lacunas, uma clarificação da aplicabilidade deste quadro normativo e o aumento da segurança jurídica." SANTOS – ***Op cit.*** 2012. p. 563.

um recurso legítimo ao uso da força, por parte do Estado agredido ou de um Estado terceiro (conceito de defesa coletiva)[826]. Importa ainda salientar que este direito está vinculado ao princípio da proporcionalidade, ou seja, a resposta à "agressão" terá que ser proporcional (sentido estrito), necessária (única hipótese possível) e adequada (os meios não devem ultrapassar os fins). Desta forma pretende-se evitar o "excesso de legítima defesa".

- As sanções coativas militares ao abrigo do Capítulo VII (art.º 42.º da CNU) surgem como *ultima ratio*, sendo aplicáveis se o CS considerar que as medidas previstas no art.º 41.º da CNU seriam ou demonstraram ser inadequadas, concretamente, com a interrupção de relações económicas/diplomáticas ou a interrupção de meios de comunicação. No entanto, também neste caso de exceção existem pressupostos. A determinação da existência de uma ameaça à paz, a rotura da paz ou ato de agressão nos termos do art.º 39.º da CNU, que as medidas provisórias e as sanções coativas não militares de acordo com os artigos 40.º e 41.º da CNU, respetivamente, não pudessem ser ou não se tenham revelado eficazes, são os fundamentos para aplicar as sanções coativas militares. À semelhança do art.º 51º da CNU, também este art.º 42º da CNU se encontra limitado juridicamente pelo princípio da proporcionalidade. Finalmente, no âmbito das medidas adotadas por organizações regionais, previstas no art.º 53.º n.º1 da CNU, salienta-se que se encontra inserido no capítulo VIII que regula as relações entre as NU e as organizações e acordos regionais. Aqui encontra-se previsto o recurso ao uso da força por parte destas últimas (a descentralização do uso da força) mas apenas quando não se conseguir alcançar uma solução pacífica das controvérsias com base no art.º 52º da CNU e, claramente, mediante autorização prévia do CS.

- O princípio da proibição do recurso à força encontra previsão na CNU, nos artigos 2.º e 3.º, bem como nas Resoluções 2625 e 3314, as quais correspondem respetivamente aos Casos "Nicarágua" e "Iraque". Nestas Resoluções é possível identificarmos os conceitos de: definição de agressão (uso ilegal da força contra a CNU); ameaça à integridade territorial; ameaça à independência política; princípio da adequação; princípio da proporcionalidade; e solução pacífica de conflitos (art.º 36.º da CNU).

Para concluir a problemática da proibição internacional do uso da força, iremos agora resumidamente abordar "a intervenção armada unilateral no Iraque, em 2003, de uma coli-

[826] No entanto, apesar de não existir uma obrigatoriedade de solicitar autorização ao Conselho para o seu uso, é necessário fazer uma comunicação imediata, assim como, as próprias "hostilidades" só se poderão manter enquanto o Conselho não tomar medidas para a manutenção ou restabelecimento da paz, momento a partir do qual este direito se extingue.

gação liderada pelos EUA, sob o pretexto de que o regime de Saddam Hussein estaria a desenvolver armas de destruição maciça"[827].

Esta intervenção armada unilateral levou a que "tivesse sido declarado o óbito do direito internacional sobre o uso da força"[828], segundo alguns autores, não obstante a própria "vigência da proibição do uso da força [ter] cessado por desuso em resultado da sua constante violação pelos Estados"[829].

No entanto, constate-se que "na Cimeira Mundial de 2005, os Chefes de Estado e de Governo dos EM das NU reafirmaram que as disposições da Carta são suficientes para responder a todo o tipo de ameaças internacionais à paz e à segurança"[830]. Com efeito, esta "prova de vida do *ius ad bellum* pós-II Guerra Mundial[831] torna crucial clarificar o âmbito e os efeitos da proibição do uso da força[832] enquanto regra fundamental para a prevenção de conflitos armados no século XXI, em particular à luz das transformações que o desenvolvimento tecnológico introduziu nos sistemas de defesa dos Estados e da emergência de novas ameaças securitárias, como o terrorismo transnacional ou a proliferação de armas de destruição maciça"[833].

No caso *sub judice* refira-se que as "intervenções armadas estaduais unilaterais podem ter lugar na sequência de autorização do CS constante de resolução adotada ao abrigo do Capítulo VII da CNU (ação em caso de ameaça à paz, rutura da paz e ato de agressão), ou resultar do exercício do direito de legítima defesa individual ou coletiva (art. 51.º da CNU), em resposta a um ataque armado"[834]. Por conseguinte, atualmente "a grande questão que os Estados enfrentam relativamente ao uso da força já não é a sua licitude. Tal como no Século XIX, apenas questionam a sua conveniência."[835]

---

[827] COUTINHO, Francisco – A Proibição do Uso da Força no Século XXI. In CALDAS, Roberto et. al. – **Guerra e Paz no Século XXI: políticas e direito internacional.** Coimbra: Almedina, 2018. p. 83.
[828] *Ibidem*.
[829] *Ibidem*.
[830] *Ibidem*.
[831] "O *ius ad bellum* (o direito internacional sobre o uso da força) esteia-se na proibição de recurso à força pelos Estados enquanto instrumento de política externa. Nos termos do art. 2.º, n.º 4, da CNU, os membros desta organização internacional devem: "abster-se nas suas relações internacionais de recorrer à ameaça ou ao uso da força, quer seja contra a integridade territorial ou a independência política de um Estado, quer seja de qualquer outro modo incompatível com os objetivos das Nações Unidas." *Ibidem*.
[832] "A proibição do uso da força constitui uma das traves-mestras da CNU. Trata-se também de uma norma que reflete direito costumeiro, com a natureza de *ius cogens*, que, a par da proteção dos direitos humanos, constitui a mais relevante conquista da ordem jurídica internacional no Século XX." *Ibidem*.
[833] *Ibidem*.
[834] "Para além destas situações, tem sido profusamente discutida a emergência de regras costumeiras que legitimariam operações militares que assumam como propósito evitar catástrofes humanitárias iminentes ou resgatar nacionais que se encontrem em perigo no território de outro Estado." COUTINHO – ***Op cit.*** p. 84.
[835] *Ibidem*.

Todavia, a "prática nas relações internacionais revela (…) que os Estados procuram justificar a necessidade de uma intervenção militar numa das exceções reconhecidas à proibição do uso da força previstas na Carta ou (…) no direito costumeiro", o que na prática manifesta o reconhecimento de uma limitação geral ao seu *ius ad bellum*.[836]

Deste modo, a "intervenção no Iraque em 2003 deve ser observada como um episódio isolado que não coloca em causa a normatividade da proibição do uso da força"[837].

Por outro lado, abrangidas na proibição do uso da força estão igualmente as situações de utilização por um "Estado de meios não convencionais que tenham a capacidade de causar diretamente, à semelhante de um ataque militar cinético (por meios convencionais), danos patrimoniais e humanos significativos noutro Estado, designadamente, através de ataques cibernéticos (v. g. a destruição de sistemas informáticos que provoque a abertura das comportas de uma barragem, a colisão entre aviões ou a fusão de um reator de uma central nuclear)"[838], entre outros.

Nos termos do art.º 2.º, n.º 4, da CNU, os EM das NU apresentam-se como os únicos destinatários da proibição do uso da força, isto é, apenas as "intervenções armadas de e contra EM estão abrangidas por esta disposição. Do direito costumeiro resulta ainda um alargamento da proibição a Estados que não integram as NU e as organizações internacionais"[839].

Neste sentido, os atores não estaduais estão, regra geral, "excluídos do âmbito pessoal de aplicação da proibição do uso da força (…), não obstante alguns destes (v. g. grupos terroristas, beligerantes ou insurretos) terem por vezes capacidade para desenvolver operações armadas equiparadas, na escala e nos efeitos, às dos Estados"[840].

---

[836] COUTINHO – ***Op cit.*** p. 85.

[837] "A violação da proibição do uso da força, para além de legitimar uma resposta militar em legítima defesa ou a intervenção armada da comunidade internacional através do CS, é suscetível de produzir efeitos em diversos regimes de direito internacional." COUTINHO – ***Op cit.*** p. 86. "No âmbito da proibição prevista no art.º 2.º, n.º 4, da Carta incluem-se tanto intervenções armadas diretas como indiretas. A definição de agressão apresenta como exemplos de ato de agressão, "a forma mais grave e perigosa do uso ilícito da força" (5.º parágrafo do preâmbulo), intervenções que envolvem o uso da força direto, através das FA do Estado agressor [art.º 3.º, alíneas a) a e)], e o uso da força indireto, através das FA de outros Estados ou de forças militares privadas (mercenários) [art.º 3.º, alíneas f) e g)]." COUTINHO – ***Op cit.*** p. 89.

[838] COUTINHO – ***Op cit.*** p. 90.

[839] COUTINHO – ***Op cit.*** p. 91.

[840] "Não é claro se a proibição do uso da força abarca ações armadas contra "Estados falhados"; isto é, Estados sem um governo efetivo. A partir de uma interpretação lógica do art.º 2.º, n.º 4, da Carta foi sugerida a redução teleológica do âmbito da proibição do uso da força, considerando-se não poder haver um uso da força contra um Estado que materialmente não existe e que, por essa razão, é incapaz de impedir a ocorrência de graves violações dos direitos humanos no seu território. Esta interpretação é, todavia, contestada com o argumento de que a exclusão do âmbito da proibição do uso da força deste tipo de intervenções humanitárias abriria a porta a práticas abusivas." COUTINHO – ***Op cit.*** p. 91-92.

Todavia, deverá ser feita "uma interpretação atualista da Carta de forma a adaptá-la à circunstância de uma das maiores ameaças securitárias globais, o terrorismo transnacional, a atuar frequentemente a partir de Estados falhados"[841]. Deste modo, o art.º 51.º da Carta prevê o "direito de legítima defesa como um direito "inerente" reconhecido aos Estados para que estes se possam defender de ataques que têm origem fora das suas fronteiras"[842], o qual terá de, em todo o caso, estar de acordo com "o princípio da necessidade e da proporcionalidade, estando à partida preenchido o requisito da necessidade em virtude de um Estado falhado não ter capacidade para resolver sozinho a ameaça terrorista que opera a partir do seu território"[843].

A violação da proibição do uso da força produz determinados efeitos, os quais analisaremos de seguida, não esquecendo que a referida proibição do uso da força é "uma norma de *ius cogens* e constitui uma obrigação *erga omnes*[844] cuja violação pode gerar múltiplos efeitos em diferentes regimes de direito internacional"[845].

Esta violação constitui um ato internacional ilícito, uma vez que "no plano da responsabilidade internacional dos Estados, uma intervenção armada que não esteja justificada por uma exceção à proibição do uso da força constitui um ato internacional ilícito [art.º 1.º dos Artigos sobre Responsabilidade dos Estados por Atos Internacionais Ilícitos (AREAII)]"[846]. Deste modo, a referida ilicitude poderá gerar um "dever de reparação pelos danos causados, o qual pode ser invocado por qualquer Estado, dada a natureza *erga omnes* da proibição do uso da força (art.º 48.º AREAII)"[847]. Já no caso de se tratar de uma "intervenção armada que viole de forma "flagrante ou sistemática" esta proibição (art.º 40.º, n.º 2, AREAII), todos os Estados têm a obrigação de cooperarem, através de meios lícitos, para pôr-lhe um fim, e estão impedidos de prestar auxílio ou assistência ao Estado responsável pela mesma (art.º 41.º AREAII)"[848].

---

[841] "Parece, aliás, estar a emergir uma prática estadual no sentido de aceitar o exercício do direito de legítima defesa contra atores não estaduais que operam a partir de Estados falhados, como o demonstram as operações militares levadas a cabo por vários Estados no território da Síria contra o autoproclamado "Estado islâmico"." COUTINHO – ***Op cit.*** p. 92.
[842] O seu exercício não pode estar dependente da prova, quase impossível em Estados falhados, de que estes Estados são responsáveis pelos atos praticados por grupos estabelecidos no seu território. *Ibidem*.
[843] *Ibidem*.
[844] Uma obrigação devida à comunidade internacional no seu todo.
[845] COUTINHO – ***Op cit.*** p. 93.
[846] COUTINHO – ***Op cit.*** p. 98.
[847] *Ibidem*.
[848] "Tal inclui, designadamente, a possibilidade da adoção de contramedidas (represálias) destinadas a obrigar o Estado inadimplente a cumprir as suas obrigações (art.º 49.º AREAII), as quais, todavia, não podem violar a proibição do uso da força [art.º 50.º, n.º 1, al. a), AREAII]." *Ibidem*.

Com efeito, a violação da proibição do uso da força produz, de igual modo, "um efeito bloqueador que impede o reconhecimento de qualquer conquista territorial"[849].

Nesta perspetiva, constate-se ainda que o uso da força poderá ser gerador de invalidades de convenções internacionais, "determinando a nulidade de convenções cuja conclusão tenha sido obtida pela ameaça ou pelo emprego da força [art.º 52.º da Convenção de Viena sobre o Direito dos Tratados entre Estados (CVDTE)] e de convenções que tenham como objeto o uso da força contra Estados terceiros (art.º 53.º CVDTE)"[850].

Para concluir, falta apenas apontar, no âmbito da "responsabilidade criminal, a possibilidade de poderem vir a ser acusados indivíduos diretamente envolvidos na decisão de recorrer à força em violação da CNU"[851], após a entrada em vigor do art.º 8.º bis do Estatuto de Roma do Tribunal Penal Internacional. Este artigo define o crime de agressão como: "o planeamento, a preparação, o desencadeamento ou a execução por uma pessoa que se encontre em posição de controlar ou conduzir de forma efetiva a ação política ou militar de um Estado de um ato de agressão que, pelo seu carácter, pela sua gravidade e dimensão, constitui uma violação manifesta da CNU"[852].

3.2.1. Definição de Agressão

Antes de mais, recorde-se que um dos fins essenciais da ONU é a manutenção da paz e segurança internacionais, bem como a adoção de medidas coletivas eficazes para prevenir e afastar as ameaças à paz, reprimindo qualquer ato de agressão ou outra rutura de paz[853].

De igual modo, recorde-se o dever dos Estados, nos termos da CNU, em resolver os seus diferendos internacionais por meios pacíficos, a fim de não pôr em causa a paz, a segurança e a justiça internacionais. Neste particular, e de acordo com a CNU, refiram-se

---

[849] "A anexação de território pela força, mesmo que seguida de ocupação de facto prolongada, não determina a transferência do título de soberania sobre o território ocupado e não pode ser reconhecida por outros Estados. Uma aplicação recente do princípio do não reconhecimento de anexações territoriais feitas pela força é a Resolução da Assembleia Geral n.º 68/262, de 27 de março de 2014, sobre a integridade territorial da Ucrânia, em que se requer aos Estados, organizações internacionais e agências especiais que não reconheçam a anexação da Crimeia pela Rússia." *Ibidem*.

[850] COUTINHO – ***Op cit.*** p. 98.

[851] COUTINHO – ***Op cit.*** p. 99.

[852] Esta alteração foi introduzida pela conferência de revisão do Estatuto do Tribunal Penal Internacional, que teve lugar em Kampala, no Uganda, de 31 de maio a 11 de junho de 2010. Entrou em vigor um ano após ter sido ratificada por 30 Estados Parte no Estatuto, devendo ser confirmada pela Assembleia de Estados Parte por uma maioria de dois terços (art.º 15.º n.ºs 2 e 3 do Estatuto). A 1 de setembro de 2017, 34 Estados tinham já ratificado a alteração, incluindo Portugal (Aviso n.º 49/2017, Diário da República n.º 92/2017, Série I, de 12 de maio), aguardando-se ainda a decisão da Assembleia dos Estados Parte. *Ibidem*.

[853] O CS, nos termos do art.º 39.º da CNU, determina a existência de qualquer ameaça à paz, rutura da paz ou ato de agressão e faz recomendações ou decide que medidas serão tomadas de acordo com os artigos 41.º e 42.º da CNU, a fim de manter ou restabelecer a paz e a segurança internacionais.

os seguintes meios pacíficos de resolução de conflitos: a negociação, o inquérito, a mediação, a conciliação, a arbitragem ou até a própria intervenção das NU.

Neste sentido, as controvérsias internacionais poderão nesta mesma ordem ser resolvidas essencialmente de duas formas principais: a via pacífica ou a via jurisdicional. Pela via pacífica os conflitos podem ser resolvidos por: negociação; inquérito; mediação; conciliação; arbitragem e bons ofícios. Já a via jurisdicional subdivide-se por sua vez em jurisdicional arbitrária e judicial.

A resolução pacífica de controvérsias surge-nos na CNU no seu art.º 33.º, onde para além da apresentação de todas estas formas de resolução de litígios nos dá a entender que o CS poderá convidar as partes a resolver o seu diferendo através de uma destas formas, não deixando de lado a possibilidade de as partes o poderem fazer por si mesmas. Por sua vez, no art.º 34º sublinha-se a posição do CS através da possibilidade de este poder investigar qualquer controvérsia.

Vejamos, de seguida, em que consistem então os seguintes meios pacíficos de resolução de conflitos: negociação; inquérito; mediação; conciliação; arbitragem e bons ofícios.

- A negociação é a forma mais simples e direta de gerir o diferendo, sendo que as próprias entidades em litígio poderão chegar a acordo. Isto é, verifica-se uma conversação entre as partes, o entendimento direto e imediato através dos canais diplomáticos adequados.
- O inquérito alega-se quando a discórdia se deve a desconhecimento dos factos praticados. Nesse sentido é elaborado um inquérito por uma entidade externa às partes em conflito. Na prática, existe a criação de comissão que vai indagar dos factos na base do conflito.
- A mediação implica também a intervenção de uma entidade externa, mas desta vez com um papel mais ativo, apresenta propostas, e propõe soluções para a resolução do litígio, as quais terão de ter a concordância das partes e a fim de se à formulação de uma solução.
- A conciliação é a resolução que assenta na criação de uma comissão em número ímpar, composta por membros indicados pelas partes em causa e pelas partes neutras que analisará em pormenor os motivos do litígio e proferirá uma solução jurídica. Será a modalidade mais formal e complexo nesta via de resolução de controvérsias, na qual a comissão que examina a questão propõe uma solução.
- Na arbitragem é constituído um tribunal *ad hoc*, com membros escolhidos pelas partes para dirimir o litígio.
- Por último, os bons ofícios implicam já a intervenção de uma entidade exterior que ainda que não participe na discussão, faz um importante esforço para colocar as partes em diálogo, ou seja, há um terceiro que tenta a conciliação entre os dois beligerantes.

Outra forma de resolução de conflitos é pela ação dos tribunais internacionais. Esta via pode ainda ser subdividida em duas possibilidades: pela intervenção de tribunais arbitrais criados para cada caso em concreto e extintos após a resolução dessa contenda específica, ou pelo recurso aos tribunais judiciais permanentes. Em relação a estes últimos destacam-se pela sua relevância o TIJ, cujo estatuto está definido na CNU, e o TPI, que está estatuído no Tratado de Roma.

Após este pequeno intróito, vamos então analisar o conceito de agressão.

A Resolução 3314 (XXIX), de 14 de dezembro de 1974,da Assembleia Geral das NU veio então definir o conceito de agressão, a qual se traduz na forma mais grave e perigosa do uso ilícito da força. Neste sentido, reafirme-se que os Estados têm o dever de não recorrer ao uso da força armada para privar os povos do seu direito à autodeterminação, liberdade e independência, ou para atingir a sua integridade territorial.

Assim, define-se o conceito de agressão como sendo "o uso da força armada por um Estado contra a soberania, a integridade territorial ou a independência política de outro Estado, ou de qualquer outra forma incompatível com os princípios da Carta"[854].

O crime de agressão foi definido na Conferência de Kampala, onde a responsabilidade criminal é somente atribuída a indivíduos que se encontrem numa posição de efetivamente exercer controlo e dirigir uma ação política ou militar de um Estado.

Atente-se que esta "disposição absorveu o art.º 1.º da definição de agressão da Assembleia Geral das Nações Unidas de 1974 − Resolução 3314 (XXIX), ao mesmo tempo que enumera vários atos que poderão qualificar como um ato de agressão, patentes no art.º 3.º da Definição − tais como a invasão, a ocupação militar e o bombardeamento pelas FA de um Estado contra outro Estado"[855].

De igual modo, o ato de agressão tem que ser dissecado no contexto do seu "caráter", "escala" e "gravidade"[856]. Tal significa que "somente se pode verificar um crime de agres-

---

[854] No seguimento desta definição, o art.º 2.º vem referir que "o uso da força armada em violação da Carta por um Estado que aja em primeiro lugar constitui, em princípio, prova suficiente de um ato de agressão…", não obstante o CS poder vir a concluir que não existem elementos suficientes para se considerar que foi cometido um ato de agressão. SARAIVA – ***Op cit.*** p. 61.

[855] SANTOS, Sofia – **O Tribunal Penal Internacional e a construção de uma ordem pública internacional**. Janus.net, e-journal of International Relations, OBSERVARE. Vol. 5. N.º 2. 2014. p. 25.

[856] "No que concerne ao "ato de agressão", os critérios de "gravidade" e "escala" foram incluídos com o propósito de não sobrecarregar o Tribunal com casos de menor dimensão enquanto o critério de "caráter" pretendia excluir casos de emprego da força cuja licitude era controversa. Contudo, os critérios "caráter", "gravidade" e "escala" que possibilitam avaliar se um ato constitui uma violação manifesta da Carta não se encontram definidos – estes últimos à semelhança do que se verifica com a determinação da existência de um ataque armado nos termos do art.º 51º da CNU, o que poderá ser problemático nomeadamente devido às divergências existentes sobre o recurso lícito ao uso da força em legítima de defesa ou no caso da ingerência humanitária." SANTOS – ***Op cit.*** 2014. p. 26.

são quando um ato de agressão constitui uma manifesta violação da Carta. Assim, embora o ato de agressão possa ser cometido apenas por um Estado, a responsabilidade por tais atos ilícitos reside no indivíduo que é responsável por tal ação estatal"[857].

Com efeito, a definição de crime de agressão reconhecida na Conferência de Kampala representa um "desenvolvimento significativo no Direito Penal Internacional; porém, inclui condicionalismos formais e materiais, suscitando estas últimas questões interpretativas que poderão dificultar a determinação da existência deste crime"[858].

Assim, o Direito Internacional atribui uma particular importância "a esta regulamentação sobre o que se considera agressão, uma vez que da sua existência dependerá a legitimidade e a legalidade de uma resposta armada de um Estado ou grupo de Estados, a título de um direito inalienável dos mesmos a uma legítima defesa"[859].

Em complemento, indique-se que o art.º 2.º da referida Resolução 3314 de 1974 constitui uma "presunção para um ato ser considerado, *prima facie*, como um ato de agressão: ter o primeiro Estado utilizado da força armada em violação à CNU"[860]. Contudo, o CS terá a possibilidade de "reverter tal presunção[861], para determinar que o ato de agressão, em resposta, não teria justificado, em razões de outras circunstâncias pertinentes, inclusive de não ter sido aquele primeiro ato de suposta agressão ou suas consequências, de uma gravidade suficiente a justificar a resposta armada"[862].

Por seu turno, o art.º 3.º vem escalpelizar alguns exemplos, de forma taxativa, de atos que se podem considerar como agressão. Atualmente, a questão será de perceber se estivermos a falar do caso de um ciberataque, se consideramos ou não um ato de agressão. Numa primeira análise, estamos inclinados a concluir que um ciberataque se constituirá como uma agressão, desde que este se destine direta ou indiretamente a afetar a soberania, integridade territorial ou independência política de outro Estado.

A definição de agressão adotada na Conferência de Kampala não contempla uma possível agressão por parte de atores não estatais, não obstante os ataques terroristas de 11 de setembro de 2001 terem demonstrado a possibilidade de tal ato poder ser cometido por

[857] SANTOS – ***Op cit.*** 2014. p. 25.
[858] "É inegável que a entrada em vigor de uma jurisdição punindo o crime de agressão constituirá uma evolução, dado que será a primeira vez que um sistema permanente de justiça penal impõe uma responsabilidade criminal pelo uso ilegal da força." SANTOS – ***Op cit.*** 2014. p. 24.
[859] SARAIVA – ***Op cit.*** p. 62.
[860] *Ibidem*.
[861] Através de um exame *a posteriori* ao uso efetivo da força armada.
[862] SARAIVA – ***Op cit.*** p. 62.

entidades não estatais, bem como a magnitude que tal ato poder assumir, comparável a um ato perpetrado por um Estado.

Outra questão pertinente prende-se com o facto do crime de agressão não se encontrar definido no Estatuto do TPI.

O facto do crime de agressão não se encontrar definido no Estatuto do TPI leva a uma impossibilidade deste órgão atuar de forma preventiva ou funcionar como mecanismo de reação, no sentido de "pôr termo à violência através da sua intervenção, colocando os responsáveis sob a sua custódia, o que se justificaria pelo facto do sistema judiciário de um Estado poder ter dificuldades de funcionamento em tempos de conflito ou mesmo na fase de reconstrução, após a intervenção internacional com recurso ao uso da força, isto é, no processo de reconciliação e retribuição penal"[863].

Deste modo, a referência ao crime de agressão consta apenas na "alínea d) do n.º 1 do art.º 5º[864] e do n.º 2 do mesmo artigo, o qual refere: "O Tribunal poderá exercer a sua competência em relação ao crimes de agressão desde de que, nos termos dos artigos 121º e 123º, seja aprovada uma disposição em que se defina o crime e se enunciem as condições em que o Tribunal terá competência relativamente a este crime. Tal disposição deve ser compatível com as disposições pertinentes da CNU."[865].

Na prática, apesar de atribuir competência sobre esta tipologia criminal, "difere o momento da eficácia dessa competência para um futuro, relativamente incerto, após o acordo quanto à definição do dito crime e às condições do seu exercício, designadamente quanto às relações entre os poderes que o TPI e o CS da ONU terão face a essa definição e ao exercício dessa competência"[866].

Com efeito, verifica-se que este crime de agressão, apesar de ser aplicável a indivíduos, acaba por tocar "profundamente a soberania do Estado em questão, já que, como "crime de chefias", se aplica exclusivamente a pessoas que ocupam posições centrais na administração estatal e que personificam a própria ideia de soberania"[867]. De igual modo, em relação à "questão da determinação da ocorrência de agressão, o cenário ainda mais se

[863] SANTOS – ***Op cit.*** 2014. p. 40.
[864] "1. A competência do Tribunal restringir-se-á aos crimes mais graves, que afectam a comunidade internacional no seu conjunto. Nos termos do presente Estatuto, o Tribunal terá competência para julgar os seguintes crimes: (...) d) O crime de agressão."
[865] ESCARAMEIA, Paula – **O tribunal penal internacional e o crime de agressão.** Lisboa: Faculdade de Direito da Universidade Católica Portuguesa, 2006.
[866] *Ibidem*.
[867] *Ibidem*.

complica quando se pretende passar tal competência do CS[868] para outro órgão, sobretudo para os Estados com poder de veto no mesmo e, daí, com controlo total sobre as decisões finais"[869].

3.2.2. "*Jus ad Bellum*" e "*Jus in Bello*"

As regras sobre o Direito à Guerra[870] ou o designado "*jus belli*" são antigas e na sua concessão esteve a ideia de diferenciar de uma forma nítida um tempo de paz e um tempo de guerra.

Com efeito, no final do século XIX, começou a destacar-se do "*jus belli*" o apelidado "*jus in bello*", isto é, as normas que iriam estar na génese do DIH, ou seja, as "normas para regular as situações em que um confronto bélico já se encontra em curso"[871]. Na prática, o DIH "é o direito que rege a maneira como a guerra é conduzida"[872], sendo puramente humanitário e visa minorar o sofrimento causado pela guerra.

Por outro lado, temos o denominado "*jus ad bellum*[873]" que se destina a regulamentar as situações de guerra, que na prática se constituem como um conjunto de normas produzidas no decorrer da história, as quais se destinam a dar "alguma clareza em situações de extrema violência, possivelmente com a finalidade de dar segurança nas relações entre os Estados"[874]. Na sua origem, um dos pontos mais importantes era a discussão sobre a "legitimidade das guerras, estudos que tinham por finalidade evitar o uso da força, que não fos-

---

[868] Todo este assunto tem que ver com os limites do Direito face à Política na cena internacional, isto é, com a possibilidade de atos do órgão essencialmente "político", o CS, virem a ser sujeitos ao escrutínio da legalidade por parte de um órgão judicial.

[869] ESCARAMEIA – ***Op cit.***

[870] Direito à guerra (de fazer a guerra, quando esta se entenda como justa). O Direito Internacional contemporâneo tolera os casos de legítima defesa real contra uma agressão armada, e a luta pela autodeterminação de um povo contra a dominação colonial. Cfr. **Dicionário Diplomático.** [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://dicionariodiplomatico.blogspot.pt/2003/11/j.html.

[871] As Convenções de Genebra são uma série de tratados formulados em Genebra, na Suíça, definindo as normas para as leis internacionais relativas ao DIH. Para um aprofundamento deste tema consultar BOUVIER, Antoine – **Direito Internacional Humanitário e Direito dos Conflitos Armados.** [Em Linha]. Williamsburg: Instituto para Treinamento em Operações de Paz, 2018. [Consult. 12 Out. 2018]. Disponível em WWW:<URL:http://cdn.peaceopstraining.org/course_promos/international_humanitarian_law/international_humanitarian_law_portuguese.pdf.

[872] "O propósito do DIH é limitar o sofrimento causado pela guerra ao proteger e assistir as vítimas da mesma sempre que possível. O direito, portanto, aborda a realidade de um conflito sem considerar os motivos ou a legalidade de recorrer à força. Ele regula somente os aspetos do conflito que são de preocupação humanitária. Isso é conhecido como *jus in bello* (direito à guerra). Suas disposições se aplicam às partes beligerantes independentemente do motivo para o conflito ou se a causa defendida por qualquer uma das partes seja justa." Cfr. COMITÉ INTERNACIONAL DA CRUZ VERMELHA – **O DIH e outros regimes legais – jus ad bellum e jus in bello.** [Consult. 12 Out. 2018]. Disponível em WWW:<URL: https://www.icrc.org/por/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm.

[873] Direito ao uso da força.

[874] SARAIVA – ***Op cit.*** p. 44.

se legitimada pelo Papa, considerado no sistema medieval como um árbitro natural entre os príncipes cristãos"[875]. Acrescente-se ainda que, segundo os teóricos do Direito Internacional clássico, o "*jus ad bellum*" era um atributo de soberania do Estado.

Em complemento, recorde-se que, de acordo com a CNU, os Estados devem abster-se de ameaçar ou usar a força contra a integridade territorial ou a independência política de outro estado (art.º 2º n.º 4º).

De seguida, vamos então abordar a evolução histórica do direito à guerra.

A designação de guerra justa na história das relações internacionais teve o seu início a partir "do esfacelamento do Império Romano, tendo sido uma introdução dos teólogos cristãos, no período conhecido como Patrística, sobretudo a partir de Santo Agostinho (354-430)"[876].

Após mais algumas evoluções, o pensamento de São Tomás de Aquino (1228-74) veio despoletar uma "corrente na qual a questão do "*justum bellum*" acabaria por integrar a doutrina oficial da Teologia Moral da Igreja Católica, segundo a qual a guerra justa poderia ser resumida, em grandes linhas, como: a) a guerra baseada numa causa justa, definida em termos éticos; b) a guerra levada a cabo com uma reta intenção[877], no curso das hostilidades; e c) aquela guerra formalmente declarada pela autoridade competente"[878].

No seguimento, e até ao século XX, viveu-se um período de "aceitação do uso da força no plano das relações internacionais, diretamente filiado na distinção entre Direito da Paz e Direito da Guerra, cuja paternidade é de Hugo Grócio"[879].

Assim, até ao início do século passado, o DIP assentou numa dicotomia fundamental entre o *ius ad bellum* e o *ius in bello*. O primeiro "representava o setor do DIP que estabelecia os termos e as condições para decretar o estado de guerra, definindo o respetivo formalismo e as partes que o pudessem fazer, assim consagrando um direito dos Estados de recorrer à força no âmbito das relações internacionais"[880]. Já o segundo observava as "normas que regulavam os conflitos armados, na convicção de que haveria uma ordem normativa no meio do caos que um conflito bélico sempre pressupõe"[881].

---

[875] *Ibidem.*
[876] SARAIVA – ***Op cit.*** p. 45.
[877] Esta retidão é expressa pelo desiderato de evitar fazer o mal e procurar, sempre que possível, fazer o bem.
[878] Sem perder de vista que as regulamentações da guerra justa se referiam ao "*orbis christianorum*", ou seja, às relações internacionais entre os príncipes cristãos, a guerra aos infiéis não mereceria quaisquer restrições, sendo, portanto, sempre um "*bellum justum*". SARAIVA – ***Op cit.*** p. 45.
[879] GOUVEIA – ***Op cit.*** 2013. p. 155.
[880] *Ibidem*.
[881] *Ibidem*.

Deste modo, a entrada no século XX veio significar a confirmação jurídico-internacional da "proscrição do uso da força, paulatinamente distribuída por quatro momentos, todos encadeados entre si, numa caminhada normativo internacional sempre crescente: a proibição do uso da força na cobrança de dívidas contratuais; a moratória de guerra no âmbito do Pacto da Sociedade das Nações; a renúncia geral ao uso da força no Pacto Briand-Kellog; e a proibição geral na CNU"[882].

Vejamos então cada um destes quatro momentos.

A proibição do uso da força na cobrança de dívidas contratuais ficou estabelecida através da designada Convenção Drago-Porter, a qual correspondeu à 2ª Conferência da Haia que decorreu em 1907.

Nesta convenção ficou estabelecida a proibição do uso da força, "através das represálias, no caso de entre os Estados haver dívidas não pagas, no âmbito de uma relação obrigacional"[883].

A moratória de guerra no âmbito do Pacto da Sociedade das Nações de 1919 vinha definir o retardamento do uso da força por três meses, a qual era definida por intervenção de instância arbitral ou judicial internacional e pronúncia do Conselho; na prática, constituía-se como a primeira limitação geral do recurso à guerra como medida de *ultima ratio*, como medida coercitiva decretada e como legítima defesa.

Esta moratória de guerra tinha como objetivo impor uma limitação processual ao uso da guerra[884] e fez parte do Tratado de Versalhes, como parte I, que carimbaria o fim da I Guerra Mundial.

Deste modo, o objetivo desta moratória passava por haver uma instância internacional que tivesse o papel da decisão de fazer a guerra. Deste modo, a mesma concebeu a "primeira limitação geral ao direito de fazer a guerra, apenas se admitindo três modalidades: (i) como medida de *ultima ratio*; (ii) como medida coercitiva assim decretada; e (iii)

[882] GOUVEIA – ***Op cit.*** 2013. p. 156.

[883] Naturalmente que se trata de "um aspeto bastante pontual no seio das relações internacionais, mas não deixou de possuir uma relevância apreciável como primeiro tratado internacional proscrevendo o uso da força, ainda que marginalmente." GOUVEIA – ***Op cit.*** 2013. p. 157.

[884] Este esquema ficaria conhecido por moratória de guerra porque, não sendo uma proscrição propriamente dita, impunha o retardamento do uso da força por três meses, com a finalidade de permitir ao Conselho pronunciar-se e fazer com que as partes em conflito chegassem a acordo, além de se admitir a força como medida coerciva ou como legítima defesa. Segundo um dos seus preceitos, "acordam todos os Membros da Sociedade que, ao surgir entre eles algum diferendo suscetível de os levar a uma rotura, se submeterão, quer a um processo de arbitragem ou a uma decisão judicial, quer ao exame do Conselho", depois se concluindo nesse preceito que "mais acordam que, em caso algum, devem recorrer à guerra antes de expirado o prazo de três meses depois da decisão arbitral ou judicial ou do relatório do Conselho." GOUVEIA – ***Op cit.*** 2013. p. 158.

como legítima defesa, traduzindo-se, em termos gerais, o Pacto da Sociedade das Nações num sistema de "retardamento" do uso da guerra"[885].

A renúncia geral ao uso da força ocorreu com o Tratado de Renúncia Geral do Uso da Força, mais conhecido por Pacto Briand-Kellog[886], celebrado em 27 de agosto de 1928, o qual consistia na renúncia substantiva geral ao uso da força, deixando de fazer parte da capacidade jurídico-internacional, e pondo termo à capacidade discricionária da guerra; a partir deste pacto, a guerra/uso da força em direito internacional passou a ser considerada ilegal.

Este Tratado veio romper em definitivo com o passado. Assim, numa das suas disposições, os Estados partes aceitavam que "o uso da força deixava de pertencer à respetiva capacidade jurídico-internacional, como desde tempos imemoriais sempre se aceitou. Verdadeiramente se fazia a diferença numa diversa evolução da questão, condenando-se explicitamente a guerra como instrumento de política internacional, ao admitir-se a guerra somente como medida de *ultima ratio*"[887].

Porém, este Tratado apresentava ainda algumas imperfeições, sendo que a principal residia no facto de, apesar de ser proibido o uso da força, o mesmo não estabelecer "qualquer mecanismo sancionatório para punir o respetivo incumprimento, o que não tardaria muito tempo que viesse a acontecer, e em larga escala, rebentando a II Guerra Mundial"[888].

A Carta das Nações Unidas veio em definitivo concretizar a proibição geral do uso da força, prescrevendo a cargo do CS os objetivos de paz e segurança internacionais e monopólio do seu uso. A única exceção atual é a possibilidade de autotutela material de legítima defesa por parte dos Estados, quando os pressupostos sejam pertinentes.

Com a CNU registou-se a proscrição geral efetiva do uso da força[889], a qual se constituiu como a proibição mais ecuménica do uso da força, bem como a defesa da soberania

---

[885] *Ibidem*.

[886] Este tratado teve como negociadores o Ministro dos Negócios Estrangeiros Francês e o Secretário de Estado Norte-Americano, respetivamente Aristide Briand e Frank Kellog, embora tivesse sido assinado por quinze Estados.

[887] "Nos termos deste tratado, o uso da força só se considerava permitido como legítima defesa ou como medida de coerção para repelir as mais graves violações do DIP, tendo este momento ficado na sua História por ter sido o primeiro de proibição geral do uso da força nas relações internacionais, ao nível substantivo, e pondo termo à competência discricionária da guerra." GOUVEIA – ***Op cit.*** 2013. p. 159.

[888] GOUVEIA – ***Op cit.*** 2013. p. 160.

[889] Apesar de se aceitar que as atribuições da ONU ultrapassam o objetivo da paz e da segurança internacionais, sem dúvida que esta é "uma das suas principais finalidades, ou não tivesse esta instituição sido criada sobre os escombros dramáticos da II Guerra Mundial. Não se pode questionar que a CNU tivesse estabelecido não apenas essa finalidade como um dos seus principais objetivos, mas sobretudo tivesse afirmado o monopólio do uso da força a cargo da ONU, a deliberar por intermédio de um dos seus órgãos, o CS." *Ibidem*.

num dos seus princípios fundamentais, afirmando que "os membros deverão abster-se nas suas relações internacionais de recorrer à ameaça ou ao uso da força, quer seja contra a integridade territorial ou a independência política de um Estado, quer seja de qualquer outro modo incompatível com os objetivos das NU".

A proibição geral do uso da força apresenta como exceções formalmente previstas as seguintes: "(i) a legítima defesa; (ii) as medidas adotadas ou autorizadas pelos órgãos competentes da ONU para manter ou restabelecer a paz e a segurança internacionais; (iii) as medidas adotadas contra anteriores Estados inimigos; e (iv) as medidas adotadas por organizações regionais"[890].

Em suma, a Carta de São Francisco, que constitui a ONU, veio concretizar a proibição do uso individual da força pelos Estados nas relações internacionais, em três situações diferentes na CNU: "1º) no art.º 2º § 3º, quando determina aos membros que resolvam suas controvérsias internacionais por meios pacíficos, de tal modo a não ameaçar a paz, a segurança e a justiça internacionais; 2º) no art.º 2º § 4º, quando determina aos membros que evitem a ameaça ou o uso da força contra a integridade territorial ou a independência política de outro Estado, constituindo a pedra angular no sistema da Carta, sendo, mesmo, considerado por muitos estudiosos como autêntica norma de "*jus cogens*"; e 3º) no art.º 51º, quando preserva o que chama de direito inerente de legítima defesa individual ou coletiva, exceção à regra geral de interdição do uso da força pelos Estados, em caso de ataque armado ou tentativa de ataque, e a título transitório, isto é, até que o CS tenha tomado as medidas que o caso requer"[891].

Com a CNU, a proibição do uso da força nas relações internacionais ficou devidamente materializada, assim como a "consequente consagração do princípio da solução pacífica das controvérsias entre os Estados"[892].

Assinale-se, de igual modo, que com a CNU o termo "guerra" deixou de ser utilizado, tendo sido substituído pela designação "uso da força". No entanto, "a proibição transcende a guerra e envolve também medidas de força de natureza breve"[893].

---

[890] "As outras hipóteses, também admitidas, foram-no apenas temporariamente, o tempo e as circunstâncias se encarregando de decretar a respetiva caducidade: o uso da força relativamente aos Estados vencidos da II Guerra Mundial rapidamente perderia a sua razão de ser; as medidas regionais nunca efetivamente poderiam obter qualquer autonomia em face do desenvolvimento da função constitucional da CNU relativamente a outros tratados de natureza militar, sobre eles prevalecendo." GOUVEIA – ***Op cit.*** 2013. p. 161.

[891] SARAIVA – ***Op cit.*** p. 48.

[892] "Deve-se atentar para o facto de que o Pacto Briand-Kellog fazia menção, no art.º 12º, ao termo "guerra", ao passo que a Carta da ONU, nos itens do art.º 2º faz menção ao "uso da força", ampliando a proibição para situações além da guerra." ROSA, Patrícia; SILVA, Carla – **O uso da força em direito internacional – legítima defesa preemptiva.** Universidade de Itaúna, [s.d.]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.publicadireito.com.br/art.ºs/?cod=a08c938c1e7c76d8. p. 5.

Atualmente verifica-se um *ius belli* residual, o que acarreta algumas consequências inevitáveis: "regulativamente, na modificação de muitas das normas do Direito Internacional da Guerra; dogmaticamente, no desinteresse em que caíram estas matérias, rapidamente substituídas por outras"[894].

Com efeito, verificamos que o "*ius belli*" se continua a basear na possibilidade do uso da força, ao abrigo do Direito Internacional, meramente numa perspetiva defensiva, segundo o direito de legítima defesa, conforme a CNU.

Em Portugal, a declaração de guerra, nos casos aplicáveis, será efetivada pelo Chefe de Estado (Presidente da República), a qual depende da iniciativa do Governo, da autorização da Assembleia da República e da audição prévia e consultiva do Conselho de Estado.

3.2.3. A Legítima Defesa

A legítima defesa[895], nos termos do art.º 51.º[896] da CNU, constitui-se como a primeira exceção à regra da proibição da ameaça ou do uso da força, qualquer que seja a modalidade do uso da força no exercício de legítima defesa individual ou coletiva. Todavia, este é um preceito legal que gera alguma imprecisão na sua interpretação, devida à sua abrangência, o que leva a que, por vezes, os Estados façam uma interpretação extensiva, e até nalguns casos, abusiva em prol dos seus interesses.

O cerne da questão está precisamente na interpretação que é dada aos elementos que devem constituir um ataque armado[897]. Desta feita, são identificados três elementos constitutivos do termo ataque armado, a saber: "a legítima defesa contra um ataque terrorista exige (…) que o ataque seja realizado como um 'ato de um Estado', o que significa que deve ser atribuível a um Estado"; "o ataque em questão tem de ser comparável à luta inter-

---

[893] DINSTEIN, Yoram – **Guerra, Agressão e Legítima Defesa.** São Paulo: Manole, 2004. p. 121.
[894] GOUVEIA – ***Op cit.*** 2013. p. 163.
[895] "A legítima defesa é aquela existente em face de uma agressão injusta e atual, de forma que o emprego da violência é o único recurso possível. Atualmente, a guerra é um ato de legítima defesa, já não é mais um ato de soberania do Estado, exercido segundo as conveniências das partes." Para um aprofundamento deste tema consultar BARRETO, Renata – **A guerra como meio de solucionar conflitos internacionais.** [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_art.ºs_leitura&art.º_id=1679.
[896] Articulado do art.º 51.º da CNU: "Nada na presente Carta prejudicará o direito inerente de legítima defesa individual ou coletiva, no caso de ocorrer um ataque armado contra um membro das NU, até que o CS tenha tomado as medidas necessárias para a manutenção da paz e da segurança internacionais. As medidas tomadas pelos membros no exercício desse direito de legítima defesa serão comunicadas imediatamente ao CS e não deverão, de modo algum, atingir a autoridade e a responsabilidade que a presente Carta atribui ao Conselho para levar a efeito, em qualquer momento, a ação que julgar necessária à manutenção ou ao restabelecimento da paz e da segurança internacionais."
[897] Ataque armado tradicionalmente significa a prática de um ato ilícito contra o regime político e a integridade territorial dos Estados, devendo tratar-se de um ataque massivo e coordenado contra um outro Estado.

estatal, na sua dimensão e efeitos"; e "exige que o ataque armado não tenha cessado, mas que esteja em curso quando o direito à legítima defesa é exercido"[898].

No que respeita aos pressupostos da legítima defesa refira-se que estes estão relacionados com a existência de um ataque armado, "noção que integra a prática de um ato ilícito contra os bens dos sujeitos internacionais, fundamentalmente pensando-se nos mais relevantes valores do ponto de vista da cena internacional, como são o regime político e a integridade territorial dos Estados"[899].

Neste particular, o "uso da expressão ataque armado no art.º 51º não é inadvertido"[900], uma vez que este assume um caráter "restritivo: o exercício da legítima defesa apenas é lícito, em conformidade com o artigo, como resposta a um ataque armado"[901].

Em relação à noção de ataque armado, "sobretudo depois de tantas evoluções tecnológicas no domínio do armamento, ela tornou-se mais difusa, fugindo dos conceitos clássicos, assim hoje podendo corresponder, mais amplamente, a qualquer operação ou ato com o efeito de infligir um prejuízo ou dano no Estado e nos seus elementos fundamentais"[902].

Contudo, "essa agressão, que tem subjacente uma ação voluntária organizada contra aqueles valores, deve apresentar-se com as caraterísticas da atualidade ou da iminência: a atualidade implica que esteja a acontecer e a iminência quer dizer que está prestes a acontecer, embora nesta hipótese não seja fácil operar a delimitação da situação que lhe antecede, que já não justifica a legítima defesa"[903].

Por outro lado, os efeitos da legítima defesa consistem na "aplicação do uso da força com o objetivo de repelir o ataque armado que está sendo perpetrado contra a respetiva vítima"[904], podendo estes efeitos se manifestarem:

---

[898] SARAIVA – ***Op cit.*** p. 59.
[899] GOUVEIA – ***Op cit.*** 2013. p. 181. e SARAIVA – ***Op cit.*** p. 57.
[900] DINSTEIN, Yoram – **The Conduct of Hostilities under the Law of Armed Conflict.** UK Ministry of Defence, The Manual of the Law of Armed Conflict. Oxford: Oxford University Press, 2004. p. 254.
[901] *Ibidem*.
[902] Neste sentido, "a Assembleia Geral da ONU aprovou uma resolução tipificando diversos casos em que tal conceito se consideraria verificado, numa listagem exemplificativa, uso da força que não é permitido à luz do novo Direito Internacional dos Conflitos Armados: a invasão ou o ataque por FA de um Estado sobre o território de outro Estado, incluindo a ocupação militar e a anexação; o bombardeamento por FA de um Estado do território de outro Estado, incluindo o emprego de quaisquer armas; o bloqueio dos portos ou das costas de um Estado pelas FA de outro Estado; o ataque por FA de um Estado contra as FA terrestres, navais ou aéreas de outro Estado, bem como contra a sua frota mercante; o uso das FA localizadas no território de outro Estado sem consentimento deste ou o prolongamento da sua presença sem esse consentimento; a permissão dada por um Estado de utilizar o seu território para empreender uma ação armada contra um terceiro Estado; e o envio de grupos ou bandos armados por parte de um Estado, ou em seu nome, praticando atos armados de gravidade equiparada à dos atos anteriormente referidos." GOUVEIA – ***Op cit.*** 2013. p. 182.
[903] *Ibidem*.
[904] GOUVEIA – ***Op cit.*** 2013. p. 183.

• subjetivamente: a "legítima defesa pode ser levada acabo pelo próprio Estado que seja destinatário do ataque armado, o que bem se explica no conceito de defesa, legítima defesa que neste caso é própria, como também pela possibilidade de ser protagonizada por Estados terceiros, que assim realizam uma legítima defesa alheia, até podendo vir a suceder institucionalmente no seio de organizações internacionais militares que têm o objetivo de estrutura ruma legítima defesa coletiva, como é o que se passa com a Organização do Tratado do Atlântico Norte, ainda que a sua criação tivesse sido contestada na comunidade internacional, a começar pela então União das Repúblicas Socialistas Soviéticas"[905];

• objetivamente: a ação de resposta em legítima defesa está "internamente limitada, ao não poder surgir fora do contexto que venha a ser recortado pelo princípio da proporcionalidade, claramente se proibindo o excesso de legítima defesa"[906];

• procedimentalmente: o "exercício da legítima defesa é sempre provisório, devendo terminar logo que o CS tome as medidas que considere apropriadas, com isso se restabelecendo o monopólio público do uso da força"[907].

Deste modo, refira-se que o direito de legítima defesa se alicerça na existência de um ataque armado perpetrado contra um Estado, o qual pode ser praticado pelo próprio Estado ou por Estados terceiros, tratando-se neste último caso de uma legítima defesa coletiva.

De igual modo, registe-se que o objetivo da legítima defesa "não é punir, retaliar, vingar, mas sim defender de um ataque injusto, atual ou iminente"[908].

Em complemento, registe-se que apesar das medidas tomadas não dependerem de uma autorização do CS, devido a legalmente tal não ser exigível, estas têm que lhe ser comunicadas de forma imediata[909], devido ao CS ser considerado como a autoridade guardiã da paz e segurança internacionais[910].

Todavia, recordemos que existem limites jurídicos para o exercício da legítima defesa, a fim de não se verificar um abuso de direito. Deste modo, mencionem-se "o respeito

---

[905] *Ibidem*.
[906] GOUVEIA – ***Op cit.*** 2013. p. 184.
[907] *Ibidem*.
[908] ROSA – ***Op cit.*** p. 12.
[909] "Importa esclarecer que a CNU possibilita o uso da força pelos Estados, em legítima defesa, mas também cuida de restringir esta prerrogativa ao exigir que os Estados comuniquem imediatamente ao CS as medidas tomadas no exercício da legítima defesa. O caráter provisório da legítima defesa pretende circunscrever o alcance deste direito: a Carta determina que este se extingue, assim que o CS das NU tenha tomado as medidas necessárias para a manutenção ou restabelecimento da paz e da segurança internacionais." VELOSO, Ana - Ação relativa a ameaças à paz, ruptura da paz e atos de agressão: art.º 51. In BRANT, Leonardo (Org.). **Comentário à Carta das Nações Unidas.** Belo Horizonte: Centro de Direito Internacional, 2008. p. 774.
[910] "Os atos praticados em legítima defesa devem ser comunicados imediatamente ao CS e só são lícitos se praticados até que o Conselho tome as medidas necessárias para restabelecer a paz e segurança internacionais." ROSA – ***Op cit.*** p. 12.

pelo princípio da proporcionalidade que se desdobra nos requisitos de proporcionalidade *strictu senso*, necessidade e adequação"[911].

Nos termos do art.º 51º da CNU, o direito de legítima defesa é encarado como um "direito inerente[912], significando que é um direito natural e fundamental do Estado, do qual depende a própria preservação do Estado, e [que] será exercido de forma regular e legítima quando determinadas condições estiverem presentes"[913].

Assim, a doutrina maioritária defende que só existe legítima defesa nos casos em que se verifique uma "situação de resposta a um ataque já ocorrido (contra o Estado em si ou contra um outro Estado que pede ajuda), tendo ainda parte considerável da doutrina e prática estatal aceite a possibilidade de legítima defesa se o ataque for iminente e não for possível ser repelido de outro modo"[914]. Em contraponto, e sem grande acolhimento na doutrina ou jurisprudências internacionais, surge a conceção de que seria possível existir uma "intervenção armada para prevenir uma possibilidade de um ataque, designadamente porque o Estado em causa se está a armar e pode ser uma ameaça"[915]. Tal, acontece "sobretudo devido aos abusos a que se presta"[916] e ao seu difícil controlo. Logo, não é viável.

No entanto, quando estamos a falar do exercício deste direito em resposta a uma situação de terrorismo, a utilização da força como legítima defesa já denota algumas dificuldades dos parâmetros de licitude, porquanto: a "legítima defesa contra um ataque terrorista exige, de acordo com o conceito tradicional do art.º 51º da CNU, que o ataque terrorista seja realizado como um "ato de um Estado", o que significa que deve ser atribuível a um Estado; além disso, o ataque em questão tem de ser comparável à luta inter-estatal, na sua dimensão e efeitos; e, por último, o art.º 51º da CNU exige que o ataque armado não tenha cessado, mas que esteja em curso quando o direito à legítima defesa é exercido"[917].

---

[911] "Por outras palavras, tem que se verificar uma correlação legítima entre a importância da intervenção e os fins perseguidos, os meios têm que ser adequados a esses fins e o ato exercido tem que ser necessário, não existindo uma alternativa mais suave ao emprego da força militar." SANTOS – ***Op cit.*** 2012. p. 538.
[912] A legítima defesa, nos termos do art.º 51º da CNU, assume-se como um "direito inerente" e que exige um ataque armado contra um Estado.
[913] O conceito de "legítima defesa – facto objetivamente ilícito cometido para repelir uma violência efetiva e injusta – tem importância nas comunidades jurídicas onde a proteção do direito é uma função exclusiva de órgãos apropriados e onde é, por conseguinte, proibido aos membros dessa comunidade fazer justiça com as próprias mãos: a legítima defesa representa então uma exceção a essa proibição." SARAIVA – ***Op cit.*** p. 55.
[914] ESCARAMEIA, Paula – **Guerra do Iraque – Fundamentos Jurídicos do Uso da Força.** Lisboa: Instituto Superior de Ciências Sociais e Políticas, Universidade Técnica de Lisboa, 2003. p. 2.
[915] *Ibidem*.
[916] *Ibidem*.
[917] SARAIVA – ***Op cit.*** p. 59.

Considerando o descrito, importará esclarecer, no âmbito da delimitação do direito de legítima defesa, as questões relativas à interpretação do conceito de "ataque armado" e à admissibilidade de medidas de caráter preventivo ou preemptivo.[918]

Neste contexto, atentemos à análise dos ataques terroristas de 11 de setembro de 2001 contra os EUA[919]. O cerne da questão destes ataques é o de serem ou não considerados como ataques armados, devido ao facto de que alguns autores frisarem que "um ato cometido por entidades não-estatais não pode ser considerado um "ataque armado" no sentido do art.º 51º, ou seja, o envolvimento de um Estado é condição imprescindível"[920].

Por outro lado, a maioria da doutrina alega que não é possível inferir do art.º 51º a "imprescindibilidade de uma responsabilidade estadual. Além disso, recorrem às resoluções 1368 e 1373 nas quais o CS qualificou os ataques terroristas de 11 de setembro de 2001 como um ataque armado para sustentarem a sua posição. Neste sentido, o jusinternacionalista alemão Matthias Herdegen frisa a necessidade de se dissociar o direito de legítima defesa de uma responsabilidade estadual"[921].

Vejamos agora a legítima defesa preventiva e a legítima defesa preemptiva.

A legítima defesa preventiva é aquela que se exerce "para evitar um risco futuro plausível, porém hipotético". Já o ataque preemptivo traduz-se numa "ação com base na prova, isto é, ameaça implícita, iminente e reconhecida de que um inimigo está prestes a atacar"[922].

Com efeito, a "legítima defesa preemptiva sustenta-se na eminência de ataque armado – que certamente se realizará – enquanto a legítima defesa preventiva baseia-se numa hipótese e, como tal, pode ou não confirmar-se"[923].

Assim, verificamos três posições discordantes em relação à licitude da legítima defesa preventiva. A primeira interpreta o art.º 51º de forma estrita, não aceitando o direito de medidas de natureza preventiva, pelo que o ataque tem de ser "atual", isto é, ou ter ocorri-

---

[918] SANTOS – ***Op cit.*** 2012. p. 544.
[919] Na prática, trata-se de "esclarecer indubitavelmente se ataques desta natureza preenchem esse requisito e, nesse caso, em que circunstâncias. Esta ausência de clareza é problemática, pense-se que, por exemplo, o uso da força por parte do novo terrorismo internacional possui caraterísticas específicas que podem ter consequências semelhantes às de ataques perpetrados por Estados." SANTOS – ***Op cit.*** 2012. p. 545.
[920] *Ibidem*.
[921] Assim, preconizam um repensar dos critérios do parecer do TIJ, pelo menos no âmbito do terrorismo internacional, dado serem demasiado restritivos. A vigência destes critérios significaria que o Estado lesado não poderia reagir, por obediência ao princípio da proibição do uso da força, enquanto o infrator estaria protegido por esta mesma disposição, mesmo quando um Estado estivesse indiretamente envolvido. *Ibidem*.
[922] RAMMINGER, Erica. **O conceito de auto-defesa na Carta da ONU e a Guerra no Iraque: Guerra preventiva ou preemptiva?** [Em Linha]. [Consult. 05 Out. 2019]. Disponível em WWW:<URL: www.cedin.com.br/revistaeletronica/art.ºs. p. 05. e ROSA – ***Op cit.*** p. 13.
[923] ROSA – ***Op cit.*** p. 14.

do ou ainda se encontrar a ocorrer[924]. Os defensores de uma "legítima defesa preventiva consideram que a expressão "no caso de ataque armado" no art.º 51º deve ser interpretada igualmente no sentido de um ataque iminente"[925]. Porém, a "posição dominante defende o critério de iminência e recusa a possibilidade de medidas preemptivas, uma vez que remetem para uma ameaça de natureza abstrata", pelo que tornar este tipo de legítima defesa "dependente de um poder discricionário estatal poderia dar origem a abusos de direito".[926]

Em complemento, e de acordo com uma análise restritiva, recorde-se que o "art.º 51.º faz menção unicamente a ataque armado. Se o artigo visasse permitir o uso da força diante da iminência de um ataque, teria sido expresso"[927].

Atualmente, a questão da possibilidade da legítima defesa preemptiva diante da iminência de um ataque alicerça-se na necessidade de se perceber se as novas tipologias de ataques possibilitam uma leitura ampliativa do art.º 51º, considerando que:

> "A escolha das armas pelo Estado atacante é imaterial. Conforme salientado pela Corte Internacional de Justiça, no seu Parecer de 1996, sobre a legalidade da Ameaça ou uso de Armas Nucleares, o art.º 51º não se refere a armas específicas; ele se aplica a qualquer ataque armado, independentemente da arma empregue. Por outras palavras, um ataque armado pode ser realizado de forma convencional ou não convencional, de forma primitiva ou sofisticada. No despertar do terceiro milénio, o que desponta no horizonte é um "ataque em rede pelo computador". Se tal agressão causasse fatalidades (resultando por exemplo no fechamento de sistemas computadorizados que controlam as redes de abastecimento de água e represas, causando a inundação de regiões habitadas), esse fato seria qualificado como um ataque armado."[928]

Deste modo, e considerando a "multiplicidade e imprevisibilidade das ameaças, é indispensável que seja alcançado um maior consenso normativo, que se deve processar através de uma reinterpretação do art.º 51º e do Capítulo VII[929].

---

[924] Nesta perspetiva, a "admissibilidade de medidas preventivas poderia conduzir a uma erosão deste direito, uma determinação de "iminência" - requisito alegado pelos defensores de uma legítima defesa preventiva - por parte do(s) Estado(s) potencialmente vítima(s) poderia conduzir a um abuso do poder discricionário, a um enfraquecimento da norma proibitiva do uso da força e a um inaceitável desvio deste princípio." SANTOS – ***Op cit.*** 2012. p. 546.

[925] "Este argumento prende-se com a irrazoabilidade do Estado, potencial vítima ter que aguardar a ocorrência de um ataque, que poderá ser aniquilador; o desenvolvimento de armas de destruição maciça encerra o perigo de estas poderem ser usadas em qualquer altura, quer por entidades estatais, quer não-estatais." SANTOS – ***Op cit.*** 2012. p. 547.

[926] "Efetivamente, esta interpretação permite responder de forma mais eficaz às novas ameaças do que uma interpretação em sentido estrito do art.º 51º. Repare-se, que um determinado ato terrorista pode não ter um envolvimento estadual implícito ou pode ser difícil apurar a responsabilidade estadual de uma forma inequívoca. Pode-se considerar esta tese como a mais adequada e lícita no âmbito dos parâmetros jurídico-internacionais, porém não permite suprir todas as incertezas jurídicas." SANTOS – ***Op cit.*** 2012. p. 548.

[927] ROSA – ***Op cit.*** p. 15.

[928] DINSTEIN – ***Op cit.*** p. 255.

[929] "Embora seja difícil que os EM ponham de parte os seus interesses nacionais ao agir no CS, esta base normativa pode aumentar a segurança jurídica relativamente ao alcance da proibição do uso da força e, por

Assim, na atualidade "o CS deve assumir um papel primordial, mais amplo e interventivo, que se desdobra em dois níveis: o CS como impulsionador e como implementador deste consenso normativo, no âmbito de uma reforma do seu modo de atuação, designadamente, fortalecimento da sua eficácia"[930].

No que respeita ao *ius ad bellum*, nos termos do Capítulo VII, deveria ser adotada uma resolução pelo CS que prescrevesse os princípios para o recurso ao uso da força. Na prática, deveriam ser "critérios catalogados, que seriam atualizados regularmente com base nas experiências reunidas, com lista de conflitos em curso anexada e definidores de uma ameaça à paz de acordo com o art.º 39º"[931], devendo ser elencada igualmente a questão do eventual uso da força no ciberespaço.

Tal, não significa o "regresso à teoria da guerra justa e respetivos critérios *ius ad bellum* no sentido clássico, mas de uma transformação da guerra justa, que assenta em critérios de decisão num processo regulamentado juridicamente"[932]. Aqui o CS deve ter um papel fundamental na qualidade de "autoridade adequada para a determinação destes critérios, avaliação sobre a existência de um direito de uma guerra justa com base nestes critérios e decisão de medidas para o restabelecimento da paz e segurança internacionais"[933].

Neste particular, o Relatório de Grupo de Alto Nível sobre Ameaças, Desafios e Mudança enuncia "cinco critérios de legitimidade: seriedade da ameaça, justo propósito, último recurso, meios proporcionais e balanço das consequências"[934].

No paradigma atual, após os acontecimentos do 11 de setembro de 2001, "deve-se estar atento às justificações para o uso da força em direito internacional, uma vez que os Estados podem desvirtuar o sentido do que estabelece a CNU considerando o estado de alerta em que se colocaram"[935].

Em resumo, poderemos afirmar que o direito de legítima defesa tem três princípios basilares, a saber: a legítima defesa pode ser individual ou coletiva, uma vez que este direito pode ser exercido pelo próprio Estado ou por Estados terceiros, tratando-se neste caso de

---

conseguinte, evitar o seu recorrente questionamento e violação. A necessidade de uma interpretação flexível desta norma assente na sua definição mais concreta, na clarificação e, mormente, na determinação rigorosa dos limites do direito de legítima defesa, do Capítulo VII e das possíveis exceções legítimas assume uma importância fundamental." SANTOS – ***Op cit.*** 2012. p. 554.

[930] SANTOS – ***Op cit.*** 2012. p. 555.

[931] SANTOS – ***Op cit.*** 2012. p. 560.

[932] SANTOS – ***Op cit.*** 2012. p. 562.

[933] *Ibidem*.

[934] SANTOS – ***Op cit.*** 2012. p. 561.

[935] Camuflar os interesses individuais dos Estados envolvidos numa controvérsia internacional, fornecendo uma pretensa justa causa – legítima defesa preemptiva – para ações que se baseiam no uso da força, significa desconsiderar os fins a que se destina a CNU. ROSA – ***Op cit.*** p. 18.

uma legítima defesa coletiva; o art.º 51º consagra o direito de legítima defesa mediante a existência de um ataque armado perpetrado contra um Estado membro das NU; e embora as medidas tomadas não dependam de uma autorização do CS, uma vez que não constitui um requisito jurídico, têm que ser comunicadas de forma imediata respeitando a sua autoridade como guardião da paz e segurança internacionais.

De modo idêntico, o caráter provisório da legítima defesa pretende circunscrever o alcance deste direito: a Carta determina que este se extingue, assim que o CS das NU tenha tomado as medidas necessárias para a manutenção ou restabelecimento da paz e da segurança internacionais.

Em complemento, constata-se que existem ainda outros pressupostos que constituem limites jurídicos a fim de não se verificar um abuso de direito, tais como, o princípio da proporcionalidade e da necessidade.

Assim, tem que se verificar uma correlação legítima entre a importância da intervenção e os fins perseguidos, os meios têm que ser adequados a esses fins e o ato exercido tem que ser necessário, não existindo uma alternativa mais suave ao emprego da força militar.

Face ao exposto, importará perceber quais serão os requisitos que interessam ter em conta para a aplicação do art.º 51.º da CNU aos casos relativos aos ciberataques, os quais poderão encontrar respaldo no Manual de Tallinn, o qual analisaremos no número seguinte.

3.2.4. Manual de Tallinn

O desenvolvimento da segurança cibernética tem levantado relevantes problemáticas legais cuja solução urge pensar, refletir e procurar normatizar.

O Manual de Tallinn[936], ou também designado como Manual de Direito Internacional Aplicável à Guerra Cibernética, surgiu da necessidade de serem estabelecidas regras internacionais básicas para a ciberguerra, tendo sido publicado sob a direção da OTAN, numa primeira tentativa de transpor as leis internacionais para a ciberguerra.

O referido Manual foi desenvolvido durante um período de três anos no Centro de Excelência em Defesa Cibernética Cooperativa da OTAN (CCDCOE) situado na capital da Estónia e foi criado em 2008, após os ciberataques de que este país foi vítima no ano anterior, os quais tinham tido como alvos o Governo, instituições financeiras e os *media* do

[936] O Manual de Tallinn está dividido em duas partes: parte I – Lei de Segurança Cibernética Internacional; e parte II – A Lei de Conflito Armado Cibernético. Para um aprofundamento deste tema consultar a obra **Manual de Tallinn: A Segurança Cibernética.** [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://agnfilho.webnode.com/news/manual-de-talinn%3A-a-seguran%C3%A7a-cibernetica-/.

país. Trata-se de um manual com 282 páginas que define as condições em que um país pode responder a um ciberataque com forças militares, e na sua elaboração estiveram mais de 40 académicos, advogados, e especialistas dos países da OTAN, pelo que não se trata de um documento oficial, mas sim de um documento que retrata as opiniões de um grupo de especialistas independentes convidado para o efeito.

Este manual, pese embora não se trate de uma lista oficial normativa, tem o condão de ser o primeiro documento orientador que define a legitimidade para a ciberguerra, tendo por base os princípios das Leis internacionais, do respeito pela soberania dos Estados e da defesa dos Direitos Humanos[937].

Considerando o âmbito do presente estudo, vamos aqui abordar a Regra 10 deste manual, a qual se refere à "Proibição de ameaça ou uso da força". Com efeito, só poderá ser realizada uma operação cibernética quando estivermos perante uma ameaça ilegal ou o uso da força contra a integridade territorial ou independência política de qualquer Estado, bem como de qualquer outra maneira inconsistente com os propósitos das NU.

Nesta perspetiva, o recurso ao uso da força apenas se pode verificar quando todos os outros meios de alcançar um objetivo legítimo tiverem falhado (necessidade) e o uso da força seja justificado (proporcionalidade) ao nível da importância do objetivo legítimo (legalidade) a ser alcançado.

O Manual de Tallinn veio na prática procurar resolver um problema que derivava da desadequada aplicação dos normativos existentes, tais como a CNU, a um ciberataque ou a qualquer conflito cibernético, no pressuposto de haver a necessidade de um qualquer Estado, por exemplo, recorrer ao uso da força para repelir uma ameaça ou um ataque, na perspetiva de legítima defesa.

De seguida, atentemos nos dois exemplos proeminentes que ilustram o significado da necessidade de interpretação dos tratados, bem como das suas deficiências, no contexto cibernético. A primeira lida com o significado da expressão "uso da força" no art.º 2.º n.º 4 da CNU, no qual se prevê a proibição desse facto. O objeto e a finalidade desta disposição eram suficientes para limitar as circunstâncias em que os Estados poderão recorrer à força para resolverem as suas diferenças. No entanto, as opiniões dos especialistas não eram unânimes para concordarem que uma ciber operação perpetrada por um Estado contra

[937] Os ataques a redes informáticas que provoquem mortes ou danos materiais significativos são algumas das situações que podem justificar uma retaliação.

outro possa causar a lesão ou a morte a pessoas, ou danos ou destruição de propriedade, e que se enquadre no contexto do uso da força[938].

O segundo caso remete-nos para o art.º 5.º da CNU, o qual prevê que os Estados possam usar a força em resposta a um "ataque armado". Aqui, o objeto e a finalidade são a garantia de que os Estados não permanecem normativamente indefesos, caso o regime de execução estabelecido na Carta não funcione como planeado. Mas a interpretação deste artigo continua a ser uma fonte de alguma incerteza e controvérsia, porque não está claro se o direito de autodefesa se estende a ataques realizados por atores não-estatais, ou se os Estados se limitam a medidas de aplicação da lei na resposta a tais atos hostis. Esta é uma questão que foi trazida para o primeiro plano do debate do Direito Internacional após os ataques do 11 de setembro contra os EUA pela *Al Qaeda*. No ciberespaço é uma questão central, porque é muito mais provável no contexto cibernético do que numa operação cinética, um grupo não-estatal ou um indivíduo terem a capacidade para lançar uma operação cibernética hostil contra um Estado, ao nível de um ataque armado, devido à relativa facilidade de adquirir os conhecimentos e equipamentos para um ataque armado cibernético em comparação com um cinético.

Neste contexto, surgem as designadas Operações de Informação (INFO OPS), as quais podem ser definidas como o "conjunto de todos os efeitos gerados de forma coordenada contra o processo de tomada de decisão de um adversário, apoiado por todas as atividades de *intelligence*, com o objetivo de o influenciar, perturbar ou destruir, enquanto simultaneamente se melhora e protege o nosso processo de tomada de decisão contra os efeitos de tais ações e contra qualquer evento involuntário ou casual"[939], sendo que, as Operações de Informação englobam um conjunto de métodos no qual se pode constatar que as "Operações sobre redes de Computadores"[940] (CNO) fazem parte. Com efeito, constata-se que as "Operações de Ciberguerra constituem-se num método para desenvolver Operações Militares, permitindo realizar guerras no ciberespaço"[941].

---

[938] VIHUL, Michael – The Nature of International Law Cyber Norms. In OSULA, Anna-Maria; RÕIGAS, Henry. **International Cyber Norms. Legal, Policy & Industry Perspectives.** Tallinn: CCDCOE, 2016. ISBN 978-9949-9544-7-6. p. 34-35.

[939] NUNES, Paulo – **Pós-Graduação/Mestrado em Guerra de Informação/Competitive Intelligence. Exercício de Gestão de Crises no Ciberespaço.** Lisboa, 4 de Junho de 2010.

[940] "A oportunidade e eficácia das Operações sobre Redes de Computadores (CNO), é proporcional à dependência do adversário dos SIC e Tecnologias de Informação. As CNO compreendem o Ataque, Exploração e Defesa de Redes de Computadores em sentido genérico." RC-OP – **Regulamento de Campanha - OPERAÇÕES**. Lisboa: Estado Maior do Exército, 2005. p. 7.

[941] PERES – ***Op cit.*** p. 2.

Deste modo, surgem as *Computer Network Attack* (CNA), as *Computer Network Defence* (CND) e as *Computer Network Exploitation* (CNE). As CNA definem-se como sendo as "medidas tomadas por meio do uso de redes de computadores para interromper, negar, corromper ou destruir informações em computadores e redes de computadores ou os computadores e as redes próprias"[942]. Já as CND podem ser descritas como sendo as "medidas tomadas por meio do uso de redes de computadores para proteger, monitorar, analisar, detetar e responder a actividades não autorizadas no âmbito dos sistemas de informação e redes de computadores"[943]. Por último, nas CNE, a "Exploração de Redes de Computadores consiste no conjunto de ações tomadas para ganhar acesso aos Sistemas de Informação (SII), explorar a informação neles residente e de uma forma geral, fazer uso, para proveito próprio, de Sistemas de Informação e Comunicação (SIC) de terceiros"[944].

Por outro lado, verificamos que o Manual de Tallinn não se ocupa do estudo de operações cibernéticas abaixo do uso do limite de força nem da criminalidade cibernética em tempo de paz. Com efeito, o seu foco está nos conflitos armados propriamente ditos, ou seja, nas hostilidades armadas que podem incluir ou estar limitadas a operações cibernéticas, de acordo com as respetivas Regras 22 e 23.

Outro apontamento necessário assenta no facto deste Manual não refletir a posição da OTAN ou de qualquer Estado, apesar de ter sido patrocinado pela OTAN, sendo o reflexo da expressão unicamente das opiniões do Grupo Internacional de Peritos, todos atuando de acordo com a sua capacidade privada.[945]

Do ponto de vista semântico, as operações cibernéticas ou operações de informação englobam os conceitos relacionados com a condução de conflitos armados. Refira-se que estas operações se consubstanciam no "emprego integrado dos principais recursos da guerra eletrónica, operações de redes de computadores, operações psicológicas, (…) e segurança de operações (…) para influenciar, interromper, corromper ou usurpar a tomada de decisões humanas e automatizadas adversas, enquanto nos protegemos"[946].

Por seu turno, as operações cibernéticas ou operações de informação abrangem as "operações de rede de computadores" (CNO), as quais envolvem, entre outros, os "ataques de redes de computadores" (CNA).

---

[942] Joint Publication 3-13. Information Operations. 2006. PERES – ***Op cit.*** p. 7.
[943] *Ibidem*.
[944] RC-OP – ***Op cit.*** p. 1-8.
[945] FREITAS, Joana – "Novas Armas, Nova Lei?": Ensaio sobre a aplicação do Direito Internacional Humanitário à Guerra Cibernética. A Problemática do Princípio da Distinção num Mundo Interconectado. In **Revista de Ciências Militares** Vol. I. N.º 2. Novembro 2013. p. 51.
[946] Tradução livre do autor. FREITAS – ***Op cit.*** p. 52.

Neste sentido, diga-se que, regra geral, existe "um CNA sempre que um CNO visa a destruição ou modificação das informações contidas na rede de computadores do adversário, a fim de enfraquecer o sistema de comunicação do adversário e / ou causar danos que extrapolam da rede alvo"[947].

Outro aspeto pertinente diz respeito a que a "maioria dos estudiosos e alguns representantes do Estado defendem que a estrutura legal existente, se aplicada por analogia, é suficiente para regular e limitar o uso de meios cibernéticos e métodos de guerra"[948].

Por outro lado, neste momento é geralmente aceite que "um CNA, embora não seja de natureza cinética, pode significar um ato de violência no âmbito do DIH[949]. Consequentemente, se um CNA se destina a, ou pode resultar em morte, lesão ou destruição, é considerado um ataque, devido às suas consequências atenderem ao requisito de violência"[950].

Deste modo, o referido Grupo de Peritos definiu ciberataques como "uma operação cibernética, ofensiva ou defensiva, que se espera que cause ferimentos ou morte a pessoas ou danos ou destruição de objetos"[951], de acordo com a Regra 30 do exposto Manual.

Considerando esta noção de ataque orientada para as consequências, "argumenta-se que o uso da guerra cibernética amplia o âmbito de operações legítimas em relação a objetos civis, que, se perpetrados pela guerra cinética convencional atingiriam o limiar da violência e, portanto, seriam ilegais"[952].

Neste contexto, importa aqui referir o princípio da distinção, segundo o qual, "apenas combatentes e objetivos militares podem ser alvos, tornando absolutamente proibido o ataque intencional a civis ou objetos civis"[953].

---

[947] "Os meios mais comuns de desempenho são cavalos de tróia, vírus, *worms* e bombas lógicas, que podem causar interrupções no *software*, *hardware* ou simplesmente uma negação de serviço (sobrecarregando a rede com informações) nos computadores ou redes de computadores do adversário." *Ibidem*.

[948] Tradução livre do autor. FREITAS – ***Op cit.*** p. 53.

[949] Segundo o argumento do professor Schmitt, o conceito de ataque deve ser visto da perspectiva das suas consequências.

[950] Tradução livre do autor. FREITAS – ***Op cit.*** p. 54.

[951] "Como exemplo de um ataque cibernético, pode-se pensar no ataque de 2010 contra uma instalação nuclear iraniana chamada Natanz, por um vírus potente conhecido como *Stuxnet*, se tivesse sido cometido durante um conflito armado. Nesse caso concreto, o *malware* manipulou a operação das centrífugas a gás de uma maneira que acabou destruindo uma parte significativa de seu equipamento de enriquecimento de urânio, atrasando-o por vários anos. Portanto, causou destruição física do objeto." *Ibidem*.

[952] Tradução livre do autor. FREITAS – ***Op cit.*** p. 55.

[953] "Corolário do princípio da distinção é a proibição de ataques indiscriminados, ou seja, ataques que não distinguem alvos civis e militares, ou porque o beligerante não está disposto a fazê-lo, ou porque os meios ou métodos utilizados são inerentemente indiscriminados, e princípio da proporcionalidade, que trata dos danos colaterais admissíveis decorrentes do ataque a um alvo militar, quando o primeiro não é excessivo, comparado com a vantagem militar direta e concreta prevista. Portanto, para serem ciberataques legais, é necessário poder discriminar e atingir apenas objetivos militares, e não causar danos colaterais excessivos em relação à vantagem militar prevista." Tradução livre do autor. FREITAS – ***Op cit.*** p. 56.

Na sequência do Manual de Tallinn surge a versão 2.0, pelo que o "Manual de Tallinn 2.0[954] é uma versão expandida da primeira versão do Manual, editado originalmente em 2013, aumentando a sua cobertura para a lei internacional reguladora da ciberguerra em períodos de paz"[955].

Esta versão mais recente procurou corrigir as muitas "deficiências e lacunas identificadas na primeira versão do Manual de Tallinn, [as quais] foram corrigidas e colmatadas nesta segunda versão. Destaca-se o facto de a abordagem ser, agora, mais ampla nesta segunda versão, abandonando o restrito âmbito dos ciberataques e abraçando o âmbito mais vasto das ciberoperações. A deficiente aproximação às operações sobre dados foi igualmente corrigida na presente versão"[956].

Deste modo, refira-se que a versão originária deste Manual focava-se "em dois assuntos distintos: o *jus ad bellum*, que regula o uso da força pelos Estados, e o *jus in bello*, a lei que regula a forma material como os Estados podem conduzir as suas operações militares durante um conflito armado, fornecendo proteção a pessoas, objetos e atividades. Para além do anteriormente referido, o Manual de Tallinn 2.0 examina os aspetos chave do DIP, regulando as ciberoperações durante o período de paz"[957].

Neste sentido, defende-se que, no âmbito das operações ciber, o uso da força apesar de normalmente ser tratado pelos "Estados, dentro da sua estratégia da salvaguarda da segurança nacional, devem, de igual modo, estar previstos os aspetos desta natureza para as situações abaixo da linha do uso da força, como por exemplo, a espionagem"[958].

Assim, a ciberguerra deverá ser interpretada como "o modo de conduzir a guerra (*warfare*) no ciberespaço, sendo para tal pertinente os seus meios e métodos, respetivamen-

---

[954] Trata-se de um "projeto resultante de um trabalho de quatro anos, efetuado por um grupo de 19 reconhecidos peritos em DIP, abordando diversos tópicos, dos quais se destacam a soberania, responsabilidade estatal, direitos humanos e as leis marítimas, aéreas e do espaço. Este Manual identifica 154 regras enquadrantes de operações no ciberespaço, devidamente fundamentadas individualmente. Apesar de ter sido elaborado por peritos, este Manual beneficiou do contributo informal, materializado através de revisões efetuadas por parceiros especialistas, de mais de 50 Estados".

[955] LIMA, Robson et al – **O Manual de Tallinn e a Regulação da Cibersegurança e Ciberguerra.** Lisboa: Instituto Universitário Militar, 2018. Trabalho de Aplicação de Grupo do CEMC 2017/2018. p. 13.

[956] *Ibidem*.

[957] *Ibidem*.

[958] "Nesta conformidade, em 2013, o CCDCOE encetou esforços no sentido de expandir o âmbito do Manual de modo a incluir matérias do DIP durante o tempo de paz", tendo o documento sido denominado de Manual de Tallinn 2.0. "Para atingir este objetivo, reuniu um novo e reforçado conjunto de peritos e especialistas, constituído por académicos e elementos com conhecimento prático do regime legal enquadrante das atividades ciberespaço". Com base na "versão inicial do Manual, estes peritos introduziram um conjunto de alterações, materializadas por uma renumeração das regras, bem como se verificou a inserção de comentários às novas regras introduzidas". LIMA – ***Op cit.*** p. 14.

te, as armas cibernéticas com os respetivos sistemas e as táticas, técnicas e procedimentos cibernéticos, pelos quais as hostilidades no ciberespaço são conduzidas"[959].

Com efeito, atente-se que "o Manual de Tallinn 2.0 assume uma importante forma de educar, sensibilizar e aconselhar os Estados sobre os pensamentos jurídicos que poderão orientar as políticas estatais de segurança em ambiente cibernético, independentemente do enquadramento não vinculativo que possui"[960]. Todavia, seria importante existir um normativo internacional enquadrador que regulasse as ciberoperações e fosse discutido e ratificado pela maioria dos Estados, a fim de o mesmo ser respeitado e, em determinados casos, assumir um procedimento sancionatório eficiente e eficaz.

Face ao exposto, algumas conclusões podem ser retiradas:

- Um ataque cibernético é um ataque que é "definido em relação às suas consequências: se um CNA pretende ou o seu resultado previsível é causar morte, lesão ou destruição, então é considerado um ataque"[961].
- A "problemática dos objetos de uso duplo é proeminente na guerra cibernética, uma vez que torres de controlo aéreo, oleodutos e gasodutos, infraestruturas de transporte e telecomunicações e muitos outros objetos de uso duplo são controlados principalmente por redes de computadores, obrigando os militares a verificar qual é o uso dado ao objeto de destino para decidir se deve ou não atacar"[962].
- Apesar de puder ser controverso, registe-se que "os ataques cibernéticos podem alcançar ganhos militares comparáveis com menos danos colaterais e sofrimento do que os ataques cinéticos convencionais, [pelo que o] seu uso (regulamentado) deve ser incentivado"[963].
- Os autores do Manual de Tallinn não encontraram "nenhum corpo jurídico relevante que fosse inaplicável às atividades cibernéticas"[964], pelo que "não é uma epifania jurisprudencial afirmar que o direito internacional se aplica totalmente às atividades no ciberespaço"[965], uma vez que as atividades cibernéticas envolvem indivíduos que usam objetos tangíveis em domínios físicos sujeitos à arquitetura normativa do direito internacional.

---

[959] LIMA – ***Op cit.*** p. 28.
[960] LIMA – ***Op cit.*** p. 29.
[961] Tradução livre do autor. FREITAS – ***Op cit.*** p. 64.
[962] *Ibidem*.
[963] "Portanto, os esforços para criar um departamento cibernético nas FA dos Estados, onde especialistas em computação possam avaliar adequadamente os efeitos de um ataque, devem ser considerados necessários." Tradução livre do autor. FREITAS – ***Op cit.*** p. 65.
[964] "Seja como for, a natureza única das atividades cibernéticas, em particular o fato de poderem ter resultados devastadores sem causar ferimentos ou danos físicos, pode levar a incertezas interpretativas." Tradução livre do autor. SCHMITT, Michael – International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. In **Harvard International Law Journal.** Vol. 54. Harvard: Harvard College, 2012. p. 37.
[965] Tradução livre do autor. FREITAS – ***Op cit.*** p. 36.

- O Manual de Tallinn 2.0 assinalou a necessidade de dar cobertura às situações da ciber-guerra em períodos de paz, através da lei internacional, pelo que atualmente se abraçou o âmbito mais vasto das ciberoperações, em detrimento do restrito âmbito dos ciberataques. Deste modo, esta versão do Manual contempla os aspetos chave do DIP, regulando as ciberoperações durante o período de paz.

3.3. Do Uso da Força no Ciberespaço

Neste último capítulo iremos analisar e aprofundar um pouco a problemática do uso da força no ciberespaço, sendo esta antecedida por um breve enquadramento relativo à ciberdefesa, bem como explicitaremos os principais princípios da guerra clássicos, a fim de compreender a forma como o uso da força é efetuado numa perspetiva mais tradicional de um conflito armado, concluindo com a abordagem ao uso da força no ciberespaço propriamente dito.

3.3.1. A Ciberdefesa

O enquadramento já exposto conduziu a que emergisse uma nova capacidade de defesa, a designada ciberdefesa.

A ciberdefesa alicerça-se em "dois processos simultâneos, um a nível nacional e outro de dependência internacional. Estes processos estão respetivamente sob a dependência do Centro Nacional de Cibersegurança e do seu homólogo internacional, um CERT"[966].

Por outro lado, a UE adotou um Quadro da Política de Defesa Cibernética em 2014, com "cinco objetivos: 1. apoiar o desenvolvimento das capacidades de defesa cibernética dos EM relacionadas com a PCSD; 2. melhorar a proteção das redes de comunicação da PCSD utilizadas pelas entidades da UE; 3. promoção da cooperação civil-militar e sinergias com políticas cibernéticas mais amplas da UE, instituições e agências relevantes da UE e o setor privado; 4. melhorar as oportunidades de treino, educação e exercício; 5. melhorar a cooperação com parceiros internacionais relevantes, tal como a OTAN"[967].

Deste modo, do ponto de vista internacional, a UE tem privilegiado "um quadro estratégico para a prevenção e estabilidade de conflitos no ciberespaço, concentrando-se na aplicação estrita no ciberespaço do direito internacional, em particular a CNU e o direito humanitário internacional"[968].

---

[966] MILITÃO – ***Op cit.*** p. 30.
[967] Tradução livre do autor. DEFENCE – ***Op cit.*** p. 21.
[968] Tradução livre do autor. DEFENCE – ***Op cit.*** p. 25.

Neste sentido, a "cooperação entre a UE e a OTAN em ciberdefesa continua a ser uma prioridade essencial no que diz respeito à garantia de sinergias entre civis e militares e da complementaridade de esforços, [pelo que] as prioridades incluem promover a interoperabilidade em termos de requisitos e padrões de defesa cibernética, fortalecer a cooperação em treino e exercícios e harmonizar os requisitos de treino"[969].

Assim, constata-se que a "aplicação do direito internacional ao ciberespaço está entre as questões mais polémicas e politizadas da segurança cibernética internacional. Na ausência de um entendimento comum das regras legais que vinculam as ações dos Estados nesse domínio, é provável que continuem disputas sobre a legalidade das operações cibernéticas dos Estados ou suas respostas"[970].

Em complemento, no campo académico, através do "Manual de Tallinn 2.0 sobre o Direito Internacional das Operações Cibernéticas"[971], tem-se verificado um esforço com o intuito de "articular as regras legais que regem as atividades cibernéticas"[972].

Noutra perspetiva, registe-se que "as democracias liberais comprometidas com o Estado de Direito abordam a questão a partir da premissa de que as atividades cibernéticas estão sujeitas ao direito internacional pré-cibernético"[973]. Por outras palavras, o direito internacional é independente da tecnologia, motivo pelo qual não há razão para excluir as atividades cibernéticas do seu âmbito, pelo que, a UE na sua Estratégia de Segurança Cibernética de 2013 se comprometeu a aplicar o direito internacional existente no ciberespaço. Da mesma forma, a Declaração da Cúpula de Gales da OTAN de 2014 reconheceu que o direito internacional se aplica a atividades cibernéticas. Esta continua a ser a posição dominante, quer nestas organizações, quer em muitos países individuais semelhantes.[974]

Deste modo, e procurando responder à aplicabilidade do direito internacional no ciberespaço, em 2013, o *Group of Governmental Experts* (GGE) da ONU, que incluía especialistas nacionais de 15 Nações, "concordou que o direito internacional, e em particu-

---

[969] Tradução livre do autor. DEFENCE – ***Op cit.*** p. 26.
[970] Tradução livre do autor. VIHUL, Liis – Direito internacional da defesa cibernética. In DEFENCE – ***Op cit.*** p. 27.
[971] O Manual de Tallinn é um guia abrangente para consultores de políticas e especialistas jurídicos sobre como o Direito Internacional existente se aplica a operações cibernéticas, o qual foi escrito por dezanove especialistas em direito internacional, sendo a segunda edição atualizada e consideravelmente ampliada do "Manual de Tallinn sobre o Direito Internacional Aplicável à Guerra Cibernética", de 2013. Este Manual assume-se como um recurso influente para consultores jurídicos que lidam com questões cibernéticas, bem como se considera a análise mais abrangente sobre como o direito internacional existente se aplica ao ciberespaço. AAVV – **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.** 2nd Ed. Cambridge: Cambridge University Press, 2017. ISBN: 9781316630372.
[972] *Ibidem*.
[973] Tradução livre do autor. DEFENCE – ***Op cit.*** p. 28.
[974] *Ibidem*.

lar a CNU, é aplicável e é essencial para manter a paz e a estabilidade e promover um ambiente de TIC aberto, seguro, pacífico e acessível"[975].

Porém, já em 2016-17, um GGE da ONU alargado de 25 Nações[976] reuniu-se e, apesar dos amplos consensos citados acima, "o direito internacional provou ser o único item de discussão que finalmente impediu o grupo de chegar a um acordo e emitir um relatório de consenso[977]. Isso foi significativo, pois, até aquele momento, a chamada abordagem ocidental – rejeitando a necessidade de um tratado cibernético – tendia a dominar a narrativa do direito internacional"[978].

Atualmente, a posição da comunidade internacional em relação à aplicação do direito internacional no domínio cibernético é de difícil identificação, não obstante, ao nível macro, ser "provável que as democracias liberais continuem insistindo na aplicabilidade da lei existente"[979], enquanto se recusam a iniciar as negociações de tratados cibernéticos.

Por outro lado, continua ainda por concretizar, ao nível da ciber diplomacia, a "aplicabilidade do Direito Internacional Humanitário às operações cibernéticas realizadas durante conflitos armados"[980], uma vez que as operações cibernéticas se manifestam cada vez mais no campo de batalha.

---

[975] "Dois anos depois, o mesmo grupo, composto por representantes de 20 Estados, afirmou essa posição. Ambos os grupos incluíram especialistas dos cinco membros permanentes do CS da ONU e os relatórios de cada um foram subsequentemente "anotados" e "bem-vindos" pela Assembleia Geral da ONU. Assim, pelo menos a partir do final de 2015, parecia haver um consenso global de que as atividades cibernéticas estavam sujeitas ao direito internacional existente, embora fosse necessário trabalho adicional para entender com precisão como o direito internacional as governava." Tradução livre do autor. DEFENCE – ***Op cit.*** p. 29.

[976] "Durante o GGE da ONU de 2016-17, a Rússia e a China não negaram a aplicabilidade do direito internacional a atividades cibernéticas, uma vez que isso contradizia diretamente a sua posição anterior. As democracias liberais no GGE da ONU, no entanto, consideraram que a oposição ao texto do relatório sobre o direito internacional prejudicou o progresso anterior. Consequentemente, não foi possível obter consenso e o quinto GGE da ONU entrou em colapso." Tradução livre do autor. DEFENCE – ***Op cit.*** p. 30.

[977] "Isso foi ilustrado com mais clareza em 2017, quando 25 especialistas governamentais que formam o Grupo das Nações Unidas de Peritos Governamentais em Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional não conseguiram concordar com o texto do relatório conjunto, devido a um desacordo sobre se certos conceitos de direito internacional se aplicariam no contexto cibernético." *Ibidem*.

[978] Tradução livre do autor. DEFENCE – ***Op cit.*** p. 29.

[979] Contudo, "para que a lei existente desempenhe um papel significativo na prevenção de conflitos cibernéticos e na garantia da paz e segurança internacionais, a simples aceitação de que a lei se aplica não será suficiente. Em particular, os Estados precisarão de articular os parâmetros de certas regras e princípios fundamentais do direito internacional de maneira mais clara."Tradução livre do autor. DEFENCE – ***Op cit.*** p. 30.

[980] Por exemplo: a "suposta manipulação de Israel do sistema de defesa aérea da Síria em 2007, como parte da Operação *Orchard* / *Operation Out of the Box*; o uso por parte da Rússia de operações cibernéticas no seu conflito armado na Ucrânia e no seu conflito com a Geórgia em 2008; e as operações cibernéticas do Reino Unido e dos EUA contra o Daesh". Todos foram governados pelo DIH, devido a tratarem-se de situações de conflitos armados internacionais ou não internacionais. Tradução livre do autor. DEFENCE – ***Op cit.*** p. 33.

Neste particular, os países que se manifestam contra a aplicabilidade do DIH "alegam que o seu apoio legitima a guerra cibernética"[981]. Como tal, ao invés de se concentrarem em como travar guerras, os Estados devem-se concentrar em evitá-las.

Porém, o decurso do tempo tem registado um decréscimo da aplicação do DIH[982], uma vez que "as situações onde o mesmo pode ser aplicado têm registado uma diminuição, não obstante o seu relevo fáctico estar longe de o tornar inútil porque as intervenções militares, à revelia dos preceitos internacionais de proscrição da guerra, se têm sucedido"[983].

Com efeito, e apesar das "divergências sobre o direito internacional, é provável que as discussões no nível multilateral continuem, [pelo que] o desafio para os Estados comprometidos com o Estado de direito será manter a atual arquitetura jurídica internacional e impedir a sua erosão"[984].

Atualmente, estamos cada vez "mais conscientes da prevalência das ameaças cibernéticas, sejam de criminosos ou *hacktivistas*, ou potencialmente patrocinados pelo Estado.

Numa perspectiva militar, os sistemas de comunicação e informação são um facilitador crítico para todos os domínios operacionais e quase todas as capacidades se tornaram dependentes da confidencialidade, integridade e disponibilidade dos sistemas baseados em TIC"[985]. Deste modo, urge implementar medidas e recursos cibernéticos apropriados para enfrentar e combater essas ameaças, pelo que, a resiliência e preparação cibernética são tarefas importantes para as operações e missões da PCSD.[986]

Para tal, o planeamento de uma ciber defesa é vital. Portanto, o primeiro princípio para garantir segurança e defesa cibernética eficaz é considerar os aspetos cibernéticos, o mais cedo possível, nos processos de planeamento e gestão de crises da UE. Logo, os

---

[981] "Essa linha de argumento ignora a realidade de que as guerras eclodem e que limites devem ser impostos às operações cibernéticas que certamente ocorrerão como resultado disso." *Ibidem*.
[982] O DIH, também designado «direito dos conflitos armados» ou «direito da guerra», é uma área do Direito Internacional Público tem por objetivo atenuar os efeitos dos conflitos armados, protegendo os que não participam (ou já não participam) nos conflitos e regulamentando os meios e métodos bélicos, ao mesmo tempo que lida com dois problemas fulcrais: a questão da guerra (uso da força) e a questão da proteção dos direitos do homem. De igual modo, regula as relações entre Estados, organizações e outros sujeitos, encontrando-se positivado em normas de tratados internacionais ou direito consuetudinário.
[983] GOUVEIA – ***Op cit***. 2018. p. 1009-1010.
[984] "Além disso, os Estados que esperam reduzir o leque de atividades cibernéticas devem estar mais abertos a aceitar as obrigações do direito internacional, como *due diligence*, restrições às suas próprias atividades cibernéticas e à exigência de respeitar a soberania de outros estados. Por fim, todos os Estados, atuando unilateralmente ou através de organizações internacionais, devem ser mais próximos quanto à sua interpretação do direito internacional no contexto cibernético, se o direito internacional tiver um efeito significativo no ciberespaço." Tradução livre do autor. DEFENCE – ***Op cit.*** p. 34.
[985] Tradução livre do autor. POWELL, Neil – Military concept for cyber defence in CSDP. In DEFENCE – ***Op cit.*** p. 35.
[986] *Ibidem*.

aspectos cibernéticos devem ser incluídos na avaliação geral de ameaças ao planear uma operação ou missão em potencial.

Deste modo, em complemento com especialistas em *inteligence*, a equipa de defesa cibernética do Estado Maior da UE (EUMS)[987] avaliará as informações fornecidas e apoiará as equipas de planeamento de operações / missões, inserindo uma narrativa cibernética nos documentos de planeamento iniciais[988]. Tal, fornece uma base sólida para um planeamento mais detalhado do Comandante da missão ou operação designado e dos seus subordinados, devendo ser ainda apoiado por informações adicionais e uma análise mais aprofundada das ameaças e riscos do ciberespaço na área de operações. O Comandante pode tomar uma decisão informada sobre a importância da defesa cibernética, definir e conseguir, no conceito de operações e no plano de operação ou missão, uma defesa eficaz contra ameaças potenciais do ciberespaço.[989]

Neste sentido, desde 2014, o Serviço Europeu para a Ação Externa "desenvolveu o Quadro de Política de Defesa Cibernética da UE, que foi o principal guia para fortalecer a capacidade e resiliência da defesa cibernética na PCSD através da introdução de uma melhor governança para as diferentes partes"[990].

No seguimento, constate-se que o cibercrime é uma das principais preocupações dos CEO's em todo o mundo. Assim, segundo a CE, "em 2016 houve mais de 4.000 ataques de *ransomware* por dia e 80% das empresas europeias sofreram pelo menos um incidente de segurança cibernética"[991]. Tal, repercute-se no impacto económico do crime cibernético, o qual tem sucessivamente aumentado.

Em complemento, não esqueçamos que durante anos, a ameaça de ser vítima de um ataque cibernético foi ignorada ou foi abordada simplesmente com soluções básicas de TI, como programas antivírus ou *anti-malware* e *firewalls*. À medida que os incidentes cibernéticos se tornaram mais evidentes, as organizações responderam com mais investimento

---

[987] Estado Maior da UE (*European Military Staff*).
[988] A inteligência de ameaças cibernéticas deve ser fornecida pelas estruturas estratégicas de inteligência da UE, com base no EEAS INTCEN, incluindo a *Hybrid Fusion Cell* e a Diretiva de Inteligência do EUMS, e suportada pela partilha de informações com outras organizações confiáveis; isso pode incluir o *hub* de informações cibernéticas da UE (CERT EU), parceiros militares, como a OTAN e, é claro, os próprios fornecedores de informações cibernéticas dos EM. *Ibidem*.
[989] Tradução livre do autor. DEFENCE – ***Op cit.*** p. 36.
[990] Tradução livre do autor. INTROINI, Enrico – Integrar a cibersegurança em missões civis da PCSD. In DEFENCE – ***Op cit.*** p. 43.
[991] Regra geral, os ataques cibernéticos não estão apenas aumentando em número, mas também em sofisticação. Ao contrário desse desenvolvimento, a conscientização e o conhecimento da segurança cibernética ainda são insuficientes. 51% dos cidadãos europeus sentem-se mal informados sobre ameaças cibernéticas e mais de dois terços das empresas não têm um entendimento básico de sua exposição a riscos cibernéticos. *Ibidem*.

em prevenção, o que significou o desenvolvimento de soluções de TI mais robustas, projetadas para manter fora de redes *malware* e outras atividades maliciosas e evitar um possível apagão total não apenas de TI, mas também possivelmente das IC[992].

Com efeito, a OTAN adotou uma política de ciberdefesa, a qual pretende fazer "face a estas ameaças, aos possíveis ataques delas resultantes e promover a cooperação dentro do sistema internacional"[993], ao mesmo tempo que dá prioridade à proteção das comunicações e dos sistemas de informação da Organização e por ela operacionalizados.

Neste contexto, e considerando as diversas formas de ciberataques, a OTAN definiu dois tipos de ataques informáticos como prioritários: "(1) a espionagem cibernética – quer de nível estratégico, quer de nível operacional – este tipo de ação pode comprometer a confidencialidade dos sistemas de informação e das informações em concreto, podendo revelar-se assim segredos e informações que poderão comprometer o Estado enquanto entidade individual; (2) a sabotagem cibernética – este modo de ataque, pode ter importantes repercussões físicas, nomeadamente em termos de infraestruturas como energia ou redes de transporte, as quais são direcionadas ou os dados manipulados de forma a minar a tomada de decisão, tanto de comando, como de controlo"[994].

Deste modo, a OTAN definiu duas prioridades no que concerne à defesa cibernética. A primeira prioridade da Organização diz respeito à proteção e à defesa das suas próprias redes, tal como acordado pelos Aliados na Cimeira decorrida no País de Gales, em 2014, apesar dos constrangimentos advenientes da sua extensão territorial[995]. A segunda prioridade tem que ver com a ajuda aos seus membros, no sentido destes desenvolverem as suas próprias capacidades de defesa cibernética. Para tal, são utilizados diversos meios e fixados vários objetivos, tais como a criação de uma estratégia de ciberdefesa[996], com o intuito da

---

[992] "Contudo, tornou-se óbvio que medidas relacionadas apenas com a segurança cibernética não são suficientes e a resiliência cibernética tornou-se um tópico importante. A ideia de resiliência é uma análise do que acontece antes, durante e depois de um sistema em rede digital encontrar uma ameaça. Ter sistemas de resiliência significa, assim, ser capaz de se preparar, suportar, recuperar-se rapidamente e aprender com ataques deliberados ou eventos acidentais no mundo *online*. A cibersegurança é, portanto, um elemento importante de resiliência; no entanto, as organizações com resiliência cibernética reconhecem que operar com segurança *online* vai muito além de apenas medidas técnicas." Tradução livre do autor. DEFENCE – ***Op cit.*** p. 53.

[993] Para tal, a OTAN adotou uma política e um plano de ação defendido e aprovado em setembro de 2014, o qual estabelece como prioridade da Organização a defesa coletiva, afirmando igualmente que, o Direito Internacional se aplica ao ciberespaço. NATO - **Cyber defence.** 2016. [Em Linha]. [Consult. 15 Out. 2018]. Disponível em WWW:<URL: https://www.nato.int/cps/en/natohq/topics_78170.htm.

[994] ALMEIDA, Cláudia – A Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço. In **III Seminário IDN Jovem.** N.º 30. Lisboa: IDN, [s.d.]. p. 281.

[995] A NATO tem de garantir que os sistemas de comunicação e informação que a Aliança utiliza para as suas operações e missões são seguros e, portanto, estão a salvo de qualquer ameaça proveniente do ciberespaço.

[996] A política da OTAN engloba assim decisões dos Aliados no que diz respeito às políticas nacionais de defesa cibernética, programas de assistência aos EM – incluindo programas de emergência. Para além disto, são

OTAN se adaptar aos desafios tecnológicos da era da globalização. A título de exemplo, refiram-se as importantes decisões tomadas na Cimeira de Varsóvia em 2016, onde os EM reconheceram o ciberespaço como um domínio da guerra[997].

Com o intuito de "combater de forma mais eficaz as ameaças e riscos provenientes do ciberespaço, a OTAN criou o NATO *Computer Incident Response* (NCIRC), que tem por objetivo a proteção das entidades da OTAN e missões; além disto, o NCIRC promove também a ajuda aos membros da OTAN a lidar com as ameaças de segurança cibernética que possam colocar em causa os seus sistemas de informação"[998].

Ao nível da prevenção, o NCIRC destaca a engenharia segura de sistemas de informação para "fortalecer o alvo", com o objetivo de reduzir as potenciais vulnerabilidades ou o "campo de ataque", fornecendo além disso um suporte contínuo, *anti-malware*. A mesma é feita através de: "(1) avaliações relativamente à vulnerabilidade dos sistemas da OTAN, incluindo testes de penetração, sendo estes, parte da avaliação e gestão de riscos; (2) exercícios de treino material educacional e notificações para os funcionários da OTAN"[999].

No sentido de materializar estas operações do NCIRC, afigura-se como "necessária uma colaboração intensa dentro da Aliança (entre agências da OTAN e os EM da mesma), mas também entre os países e agências da Organização e países terceiros (não pertencentes à OTAN), organizações intergovernamentais, como a UE, autoridades nacionais responsáveis pela aplicação da lei, indústria privada ligada ao negócio da tecnologia e o mundo académico em geral"[1000].

Já em Portugal, em 2013, foi aprovado o atual Conceito Estratégico de Defesa Nacional (CEDN), aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 21 de março, o qual veio antecipar como grande tendência no ambiente de segurança global, o

definidas políticas de consciencialização, educaçãoe formação, incentivando as iniciativas de cooperação entre países e Organizações Internacionais. ALMEIDA – ***Op cit.*** [s.d.]. p. 282.

[997] "Nos termos do art.º 3.º do Tratado de Washington, os Estados têm responsabilidade de defender e desenvolver a sua plataforma nacional de segurança no ciberespaço, a fim de se protegerem os interesses dos EM, mas também da própria Organização. Além disso, os EM presentes em Varsóvia comprometeram-se a melhorar a troca de informações e medidas de auxílio mútuo na prevenção, mitigação e recuperação de ataques cibernéticos, provendo-se desta forma uma maior e melhor cooperação entre Estados." KRUPCZYNSKI, M. – **NATO's Reaffirmed Commitment to Cyber Security.** 2016. [Em Linha]. [Consult. 15 Out. 2018]. Disponível em WWW:<URL: http://futurenato.org/articles/natos-reaffirmed-commitment-to-cyber-security/.

[998] ALMEIDA – ***Op cit.*** [s.d.]. p. 282.

[999] *Ibidem*.

[1000] "Esta interligação entre os diversos atores do sistema internacional fomenta a robustez das capacidades do NCIRC, mas torna a cooperação crucial para a defesa do ciberespaço da OTAN, (…) pois estamos perante ameaças que podem desencadear um conflito generalizado." ALMEIDA – ***Op cit.*** [s.d.]. p. 283.

potencial devastador dos ataques cibernéticos, identificando o ciberterrorismo e a cibercriminalidade como ameaças e riscos prioritários.[1001]

Deste modo, o atual CEDN reconhece estes desafios de segurança do ciberespaço, pelo que preconizou a edificação ao nível das FA de uma capacidade de Ciberdefesa[1002], tendo por base a Comunicação Conjunta ao PE, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões, apresentada pela CE e pela Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, relativa à Estratégia da UE para a Cibersegurança, de 7 fevereiro de 2013, e que estabelece como prioridade estratégica desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da PCSD.

Com efeito, através do despacho n.º 13692/2013[1003], de 11 de outubro de 2013, foi determinada a publicação da diretiva iniciadora com a orientação política para a ciberdefesa, anexa ao referido despacho e que dele faz parte integrante. Assim, nos termos do referido anexo é referida a orientação política para a ciberdefesa, a saber:

a) "O ciberespaço é por natureza um espaço aberto desprovido de fronteiras tangíveis, onde tanto o setor público como o privado, civis e militares, atores nacionais e internacionais interagem em simultâneo e de forma interdependente e interligada. Por essas razões, não é um espaço seguro e protegido, sendo vulnerável a ataques cibernéticos, que podem ter como consequência perdas relevantes no plano económico e social ou constituir uma ameaça séria à Defesa Nacional (DN), quer no plano da degradação ou destruição de infraestruturas críticas quer no plano da neutralização ou negação ao acesso a recursos informacionais"[1004].

b) "Estas dependências, conjugadas com o crescente poder disruptivo e destrutivo dos ataques lançados através da internet e das redes com esta interligadas, exige o levantamento de estruturas especializadas no âmbito da ciberdefesa e obriga a DN a adotar respostas concertadas e articuladas, tanto no plano nacional como internacional."

[1001] Estas "ações têm como alvo redes indispensáveis ao funcionamento da economia e da sociedade da informação globalizada, constituindo por isso, riscos e ameaças prioritários que se replicam e multiplicam diretamente no plano interno", pelo que "representam uma ameaça crescente sobre IC, cujos efeitos e impactos podem provocar o colapso da estrutura tecnológica da organização social e económica do País". Despacho n.º 13692/2013. **Diário da República II Série.** N.º 208 (28-10-2013). p. 31976-31977.

[1002] As orientações específicas da Reforma "Defesa 2020", decorrentes da Resolução do Conselho de Ministros n.º 26/2013, de 19 de abril, prevêem o levantamento da capacidade de Ciberdefesa nacional, e preconizam em concreto a criação de um Centro de Ciberdefesa, no âmbito do Estado-Maior-General das FA.

[1003] Despacho n.º 13692/2013. **Diário da República II Série.** N.º 208 (28-10-2013). p. 31977.

[1004] Compreende-se assim, que o ciberespaço constitua um novo domínio operacional, onde podem vir a ser conduzidas operações militares e onde o levantamento de mecanismos de proteção e defesa obedece à mesma lógica e fundamentos que caraterizam a Segurança e a Defesa do Estado.

c) "A Orientação para a Política de Ciberdefesa tem por finalidade determinar os princípios essenciais, definir objetivos e estabelecer as correspondentes linhas orientadoras dos esforços a desenvolver, no âmbito da DN, visando, nomeadamente, o levantamento da capacidade nacional de Ciberdefesa."

d) A definição dos objetivos e a determinação das linhas de ação da Política de Ciberdefesa Nacional obedecem a determinados pressupostos, entre os quais: "o ciberespaço, pela sua importância para a afirmação da Soberania Nacional, constitui um espaço de defesa de valores e interesses, materializando uma área de responsabilidade coletiva"; o "ambiente do moderno campo de batalha é cada vez mais descontínuo e multidimensional, constatando-se que as operações militares têm vindo progressivamente a incluir o desenvolvimento de operações em redes de computadores, juntando aos tradicionais espaços de atuação (terra, mar e ar) também o ciberespaço"; as "atividades de Ciberdefesa são orientadas para atender às necessidades da DN visando assegurar a utilização do espaço cibernético, impedindo ou dificultando o seu uso contra os interesses nacionais"; a "segurança dos SIC constitui a base para a defesa do ciberespaço"; o "desenvolvimento tecnológico associado ao levantamento da capacidade de ciberdefesa deve ser equacionado em harmonia com o Planeamento de Defesa Militar"; e a "eficácia das ações de defesa do ciberespaço depende, fundamentalmente, da atuação sinérgica e colaborativa da sociedade portuguesa, envolvendo não apenas os órgãos do Ministério da DN, do Estado-Maior-General das FA (EMGFA) e dos Ramos, mas também a comunidade académica, os setores público e privado e a base industrial de defesa".

e) De igual modo, a Ciberdefesa deve ser regida por determinados princípios, dos quais elencamos os principais: "a capacidade de ciberdefesa deve ser estruturada e desenvolvida de forma a prevenir e retardar a rápida progressão dos ciberataques, garantindo a sua deteção antecipada, implementando ferramentas de vigilância e alerta avançado, procurando deste modo conter e limitar potenciais danos[1005]"; os "ataques cibernéticos podem ter como consequência perdas relevantes no plano económico, de vidas humanas ou constituir uma ameaça séria à DN[1006]"; as "ações e operações militares conduzidas no âmbito da ciberdefesa são executadas no respeito do quadro legal em

[1005] "O aumento exponencial do volume e sofisticação das atividades cibernéticas com fins maliciosos, bem como a velocidade com que os eventos decorrem no ciberespaço, reforçam a necessidade de atribuir especial prioridade à prevenção e contenção dos efeitos dos ataques."
[1006] "Neste contexto, através da avaliação das consequências da atividade cibernética hostil, deverá existir a flexibilidade operacional necessária para ajustar, de forma proporcional, a resposta a cada tipo de ataque e situação."

vigor, obedecendo à mesma lógica e fundamentos que caracterizam a Segurança e a DN"; as "atividades de ciberdefesa, constituindo uma área ligada às operações militares, devem por essa razão também complementar a implementação dos requisitos destinados a proteger a confidencialidade, integridade e disponibilidade dos SIC[1007], devendo para esse efeito manter-se permanentemente atualizadas e em conformidade com esses requisitos"; "uma capacidade operacional de ciberdefesa envolve o conhecimento e os recursos necessários para prever, influenciar ou bloquear as ações que potenciais adversários venham a desenvolver no ciberespaço, antes e durante as operações militares[1008]"; a "informação relativa à ciberdefesa, como sejam os detalhes relativos a ataques cibernéticos específicos, as avaliações de ameaças e vulnerabilidades, deverá ser classificada, manuseada e acedida conforme as determinações de segurança em vigor"; a "dinâmica e complexidade do ciberespaço exigem uma adaptação contínua à envolvente operacional, colocando às FA o desafio adicional de recrutar e reter o pessoal mais qualificado, capaz de integrar os requisitos inicialmente estabelecidos e, proativamente, promover a inovação e a evolução constante tanto do nível de conhecimento, competências e técnicas, como da própria doutrina de emprego operacional das capacidades"; e "só uma aproximação conjunta e cooperativa permitirá enfrentar as ameaças cibernéticas de forma a melhorar a cibersegurança e garantir a ciberdefesa de forma sustentável[1009]".

f) Os objetivos da Política de Ciberdefesa consubstanciam-se em: "1) garantir a proteção, a resiliência e a segurança das redes e dos SIC da DN contra ciberataques; 2) assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional; e 3) contribuir de forma cooperativa para a cibersegurança nacional".

g) No que respeita à Estrutura de Ciberdefesa Nacional, o "Centro de Ciberdefesa, na dependência do Chefe do EMGFA, constitui o órgão responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas".

[1007] Criptografia, segurança da informação, segurança física e do pessoal.

[1008] "Neste contexto, para avaliar o espectro da ameaça, identificar potenciais atacantes e as suas intenções, as FA devem dispor de uma capacidade de recolha e análise de informações no ciberespaço, capaz de permitir, em tempo, uma resposta eficaz. Deverão ainda dispor de competências do foro jurídico, indispensáveis na condução de operações neste domínio."

[1009] "As técnicas utilizadas pelos atores ou agentes perpetrantes são muitas vezes semelhantes e procuram explorar vulnerabilidades genéricas, comuns à maior parte das redes e sistemas."

h) A capacidade de ciberdefesa deverá ser planeada no sentido de "integrar as operações no ciberespaço no âmbito das capacidades militares"[1010], pelo que, a "defesa contra as ameaças cibernéticas deve incluir o reforço da proteção das redes, a monitorização e análise dos padrões de tráfego, a deteção precoce de ataques e a resposta aos mesmos, envolvendo para esse efeito, sempre que necessário, a condução de operações no ciberespaço".

i) A ciberdefesa deverá ter a capacidade para conduzir operações militares em redes de computadores. Para tal, deverá desenvolver "a capacidade militar para conduzir todo o espetro de operações no ciberespaço (defensivas, de exploração e ofensivas), desenvolvendo e mantendo atualizada a doutrina de emprego das capacidades associadas à ciberdefesa, e definindo os princípios básicos que orientam a criação de legislação e normas específicas de apoio às atividades da DN no ciberespaço".

j) De igual modo, deverá ser incrementada a capacidade de informações no ciberespaço, uma vez que é essencial ter a aptidão para "avaliar a dinâmica das ameaças e perceber as possibilidades e intenções de potenciais atacantes[1011]", no sentido de constituir uma "precondição para a proteção das infraestruturas de informação e para a condução de operações no ciberespaço".

k) Em relação aos atores envolvidos na DN, estes "necessitam assim de reforçar a sua capacidade de recolha e análise de informações no ciberespaço e de integrar, em tempo oportuno, a informação obtida na condução das operações de ciberdefesa, devendo ainda ter a capacidade para bloquear e anular as atividades de informações conduzidas por terceiros[1012]".

l) A partilha da informação de ciberdefesa permitirá concretizar a prevenção e a minimização dos efeitos causados por ataques cibernéticos, à qual deveremos aliar a "existência de um sistema de alerta imediato e da atualização permanente do panorama sobre as atividades maliciosas a decorrer no ciberespaço[1013]".

[1010] "Para o efeito, incorporar no Processo de Planeamento de Defesa Militar, em conjugação com o *NATO Defence Planning Process* (NDPP) e com o *Capability Defence Plan* (CDP) da UE, o desenvolvimento da capacidade nacional de ciberdefesa."

[1011] "Um desafio complexo, que se coloca no contexto cibernético, é a atribuição da origem e a identificação dos atores responsáveis pelos ataques ou tentativas de ataque."

[1012] "Neste âmbito, devem ser capazes de avaliar a evolução das ameaças cibernéticas, através da realização periódica de avaliações de ameaças à ciberdefesa e de outros relatórios especializados."

[1013] "Constituindo a ciberdefesa uma área onde se torna necessário promover sinergias e potenciar o seu emprego dual (civil-militar), deverá desenvolver-se um sistema de partilha de informação aos vários níveis e patamares de decisão, procedimentos de alerta imediato em apoio aos objetivos definidos e de colaboração com a rede nacional de serviços de resposta a incidentes de segurança informática (CSIRT), instituições privadas, universidades e organizações internacionais como a OTAN e a UE."

Por outro lado, o "ambiente do moderno campo de batalha é cada vez mais multidimensional e descontínuo, observando-se que as operações militares se foram alargando progressivamente a áreas tradicionalmente não militares"[1014]. Deste modo, as FA da "era da informação dependem, cada vez mais, da utilização do ambiente de informação e do próprio ciberespaço para conduzir todo o espectro das operações"[1015].

No âmbito militar e estreitamente ligadas ao conceito de ciberdefesa, surgem "as Operações no Ciberespaço, ou *Computer Network Operations* (CNO), incluindo no seu âmbito ações de natureza defensiva, de exploração das capacidades dos possíveis adversários ou mesmo de resposta ofensiva. A nível internacional, diferentes Nações e organizações têm vindo a adotar este conceito e estão atualmente a envidar esforços para obter as capacidades necessárias à sua implementação"[1016].

Neste sentido, na doutrina do Departamento de Defesa dos EUA[1017], o Estado-Maior Conjunto indica, dentro da Doutrina de Operações de Informação, que as capacidades CNO se compõem de[1018]:

• *Computer Network Defense* (CND), que "inclui as medidas adotadas através da utilização de redes de computadores para proteger, controlar, analisar, detetar e responder a atividades não autorizadas nos sistemas de informação e comunicações. Estas ações não procuram apenas proteger os sistemas amigos de um adversário externo, mas também contemplam a possibilidade de a sua exploração ocorrer a partir do interior da própria organização".

• *Computer Network Exploitation* (CNE), que "integra as capacidades de recolha de informações (*intelligence*) levadas a cabo através do uso de redes de computadores para recolher dados das redes de comunicações e dos sistemas de informação de um potencial adversário".

• *Computer Network Attack* (CNA), que compreende as "ações desenvolvidas através da utilização de redes de computadores para interromper, negar, degradar ou destruir a informação tratada pelas redes de comunicações e pelos sistemas de informação (do possível adversário), ou dos próprios sistemas de informação e comunicações amigos".

Face ao exposto, e de acordo com a "tendência crescente para o aumento da capacidade disruptiva e destrutiva das ciberameaças, tanto a nível internacional como nacional, os países mais desenvolvidos têm vindo a desenvolver e a reforçar a sua capacidade nacio-

---

[1014] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** 2013. p. 12.
[1015] *Ibidem*.
[1016] *Ibidem*.
[1017] *US DoD – United States Department of Defense*.
[1018] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** 2013. p. 12.

nal de ciberdefesa, explorando assim, de forma sinérgica e cooperativa, as capacidades existentes nas suas FA"[1019].

Assim, surgiu a necessidade da adoção de uma Estratégia de Segurança da Informação no Ciberespaço, devido ao "extraordinário desenvolvimento das TIC tem convertido o ciberespaço num recurso vital para o funcionamento das modernas sociedades, porque, por um lado, promove e simplifica a relação entre cidadãos, AP e empresas e, por outro, constitui um elemento básico para a prestação de serviços essenciais à comunidade"[1020].

Nesta perspetiva, a Organização para a Cooperação e Desenvolvimento Económico (OCDE) considera a internet como um "elemento essencial para promover o desenvolvimento económico e bem-estar social, assim como para fortalecer a capacidade das sociedades para melhorara qualidade de vida dos seus cidadãos"[1021].

De igual modo, Portugal considera a "Estratégia da Informação e a Segurança do Ciberespaço" como um vetor estratégico estruturante da revisão da sua Estratégia Nacional de Segurança e Defesa, considerando que "reconhece a importância de proteger e defender o processo de geração de valor associado ao desenvolvimento do potencial estratégico nacional neste domínio."[1022]

Tal, assenta na premissa que o "aumento exponencial da atividade no ciberespaço trouxe também um aumento da sua utilização maliciosa e dos incidentes de segurança"[1023].

Por este motivo, os "governos e organizações internacionais têm demonstrado uma preocupação crescente pela segurança do ciberespaço, o que se materializou na publicação, por parte de muitas nações, das respetivas Estratégias Nacionais de Cibersegurança"[1024].

[1019] "No caso de Portugal e Espanha, a cooperação com as estruturas da OTAN e da UE tem vindo também a ser explorada, de forma a defender os interesses nacionais e a fazer face ao espectro global das ameaças emergentes no ciberespaço." *Ibidem*.

[1020] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** 2013. p. 13.

[1021] "A Cibersegurança não é um mero aspeto técnico de segurança, mas a pedra angular da nossa sociedade e do sistema económico. Dada a importância crescente dos sistemas informáticos na economia, a estabilidade e prosperidade económica do país dependerá em grande medida da segurança do nosso ciberespaço." *Ibidem*.

[1022] *Ibidem*.

[1023] Em particular, os ataques de natureza intencional têm sofrido um aumento significativo ao longo dos últimos anos, demonstrado, nomeadamente, pela utilização cada vez mais frequente da internet com o propósito de mobilização social ou protesto político e, acima de tudo, pelo surgimento e desenvolvimento de uma autêntica indústria de produção e exploração de código malicioso (*vírus*, *trojans*, criação e operação de *botnets*, etc.), caraterizada por um elevado nível de especialização e cujos benefícios económicos são substancialmente maiores que o tráfico mundial de marijuana, cocaína e heroína. *Ibidem*.

[1024] A título de exemplo, mencionamos os documentos elaborados pelos governos dos EUA, Canadá, Japão, Reino Unido, Alemanha, França e Holanda. De igual modo, "no âmbito multinacional, diferentes organizações como a União Internacional das Telecomunicações, a OCDE ou a OTAN têm redigido documentos que refletem as respetivas posições sobre a segurança das redes de comunicações e do próprio ciberespaço. No âmbito militar, na sequência da aprovação em 2009 de um Conceito de Operações em Redes de Computadores, o Estado Maior da UE (EUMS) desenvolveu também um Conceito de Ciberdefesa que foi aprovado pelo Conselho da UE." INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** 2013. p. 14.

Deste modo, a OTAN definiu a ciberdefesa como uma prioridade estratégica para a Aliança, pelo que o novo Conceito Estratégico da OTAN[1025] declara expressamente que "a crescente sofisticação dos ciberataques requer o desenvolvimento urgente de uma capacidade de proteção da Aliança contra este tipo de ataques pois, como se tem vindo a comprovar, dela depende a sua própria segurança"[1026]

Assim, a NC3A[1027] considerava que a ciberdefesa se podia definir como "a aplicação de medidas de segurança para a proteção e resposta a ciberataques lançados contra as infraestruturas TIC, requerendo uma capacidade de preparação, prevenção, deteção, resposta, recuperação e extração de lições aprendidas a partir dos ataques que podem afetar a confidencialidade, integridade e disponibilidade da informação, assim como os recursos e serviços dos sistemas de TIC que a processam"[1028].

Neste contexto, surge a necessidade de "implementar os aspetos de exploração e de ataque das capacidades de ciberdefesa de um atacante"[1029]. Com efeito, poderemos referir diversas "iniciativas em diferentes países, orientadas para a criação e estruturação de um Cibercomando Militar ou o de um Ciberexército, dos quais se salientam: EUA[1030], Reino Unido, China, Rússia, Irão, Índia, Paquistão, Coreia do Norte, Coreia do Sul, Israel e, muitos mais"[1031].

Deste modo, os Estados têm operado uma alteração concetual, na qual "estão a substituir os convencionais soldados por técnicos especializados na internet, levando a uma mudança de paradigma, inerente à indissociabilidade dos ciberconflitos relativamente aos conflitos tradicionais"[1032].

[1025] Aprovado na Cimeira de Lisboa que ocorreu em 18 e 19 de novembro de 2010.
[1026] Em 8 de junho de 2011, os Ministros da Defesa dos países membros, aprovaram a revisão da Política de Ciberdefesa da NATO, estabelecendo desta forma uma visão clara para os esforços a desenvolver no contexto da edificação de uma capacidade de Ciberdefesa cooperativa da Aliança. INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** 2013. p. 35.
[1027] *NATO Consultation, Command and Control Agency*.
[1028] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** 2013. p. 35.
[1029] "Surgem assim os conceitos de ciberguerra e ciberexército, bem como o desenvolvimento de regras de empenhamento específicas que permitam não só defender mas também, se necessário, passar ao ataque." INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** 2013. p. 36.
[1030] "O Cibercomando Militar dos Estados Unidos é seguramente aquele que dispõe de um corpo doutrinário mais avançado e conceptualmente elaborado, além de ser o que, com mais transparência, reflete o progresso na implementação das suas capacidades."
[1031] INSTITUTO DA DEFESA NACIONAL – ***Op cit.*** 2013. p. 36.
[1032] "A consciencialização de que existe hoje em dia um novo vetor da guerra – a ciberguerra – juntamente com os tradicionais mar, terra, ar e espaço, deverá suscitar a obtenção de novas capacidades, que permita criar forças nesta vertente. Os atores que não desenvolvam esforços neste domínio serão suplantados pelos seus adversários, ficando em desvantagem face ao atual ambiente caraterizado por uma forte competição." SILVA – ***Op cit.*** p. 8.

Em Portugal, existe um Centro de Ciberdefesa no EMGFA. Porém, Viegas Nunes[1033] afirma que "mais do que guerra, temos assistido a ciberconflitos. Segundo a nossa Constituição, quando é guerra compete às FA intervir, mas neste caso o que se assiste é a um ciberconflito permanente e não há reivindicação do ataque"[1034].

Neste sentido, a cibersegurança deverá ser assegurada pelas FS, em particular as áreas do cibercrime e do ciberativismo, ao passo que o SIS deverá ser responsável pelo ciberterrorismo e ciberespionagem. Já as FA serão as responsáveis pela ciberdefesa. Nesta perspetiva, todas estas diferentes entidades desenvolveriam na sua esfera de atuação, esforços para prevenir, detetar, defender e recuperar face a ciberataques[1035].

Este modelo encontra suporte legal na CRP, considerando que no n.º 2 do seu art.º 273.º se encontra prescrito que "a defesa nacional tem por objetivos garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações, contra qualquer agressão ou ameaça externas". Estabelecendo um paralelismo com o contexto do ciberespaço, podemos inferir que caberá às FA assegurador a ciberdefesa nacional. Em complemento, o n.º 1 do seu art.º 272.º preceitua que "a polícia tem por funções defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos". Já o n.º 3 deste artigo refere que "a prevenção dos crimes, incluindo a dos crimes contra a segurança do Estado, só pode fazer-se com observância das regras gerais sobre a polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos".[1036]

Todavia, não obstante o citado enquadramento legal, o referido modelo carece ainda do desenvolvimento de determinadas capacidades, uma vez que "ao nível dos Ramos das FA, as capacidades de ciberdefesa cingem-se quase exclusivamente à sua própria proteção, não existindo uma doutrina comum de emprego conjunto para criar sinergias adicionais a nível da defesa nacional"[1037].

[1033] Coronel Responsável pela Repartição de Coordenação de Projetos da Direção de Comunicações e Sistemas de Informação do EMGFA.

[1034] SÉNECA, Hugo – A guerra não acabou. Nem vai acabar. In **Exame Informática.** Fevereiro de 2017. p. 66.

[1035] "Insurgentes que procurem pontos vulneráveis num determinado país irão certamente procurar vulnerabilidades na sua infraestrutura de informação, como aconteceu na Estónia em 2007 e na Geórgia em 2008. Um ataque com um grau de severidade similar ao que sofreu a Estónia em 2007, não só é possível de ocorrer em Portugal, como deveria ser equacionado com objetividade." SILVA – ***Op cit.*** p. 15.

[1036] *Ibidem*.

[1037] Por outro lado, "o setor privado possui a infraestrutura do ciberespaço, pelo que se torna essencial no desenvolvimento de uma estratégia de cibersegurança nacional, assumindo-se como um ator importante no desenvolvimento das capacidades de ciberdefesa, as instituições académicas. Neste contexto, torna-se importante estabelecer parcerias público-privadas, efetuando a sua integração com as estruturas militares, na cria-

De igual modo, "uma estratégia de cibersegurança deverá estar assente em dois pilares sólidos: o livre fluxo de informação e um robusto relacionamento internacional[1038], [o qual] deverá compreender a partilha das capacidades de aviso prévio e de boas práticas identificadas, num esforço de desenvolvimento de capacidades e de treinos conjuntos"[1039].

Face ao exposto, a ciberguerra assume-se como uma "nova categoria criada para que se pudesse analiticamente analisar a metodologia de ação de uma guerra perpetrada num novo 'campo de batalha' o ciberespaço"[1040]. Saliente-se que, a "ciberguerra surgiu num mundo já dominado pela Guerra da Informação, em que o mais valioso não são as ligações, mas a informação contida nessas ligações ou que é difundida através das mesmas"[1041].

Constate-se que a ciberguerra teve o condão de "alterar o paradigma existente da Guerra, as suas pedras basilares foram os estrondosos avanços tecnológicos e as capacidades que advieram da utilização do amplo meio que é o ciberespaço. Esta 'nova guerra' surge com caraterísticas muito próprias que a dotam de um poder de destruição único"[1042].

Contudo, não poderemos confundir os conceitos de ciberguerra e de ciberterrorismo, uma vez que são distintos. Assim, "enquanto o primeiro se refere a uma ação de amplo espectro e cuja dimensão objetiva é atingir a maior dispersão espacial e de danos[1043], o segundo conceito é projetado, visando atingir fins políticos cujos alvos estão espacialmente e temporalmente confinados"[1044].

Em termos práticos, a ciberguerra é "uma guerra[1045] assimétrica que pode decorrer de forma irregular, ou seja, os seus intervenientes adotam regularmente métodos de ação definidos como atos extremos[1046] e desproporcionais em relação aos outros. Com o fenómeno da globalização, a capacidade de provocar uma guerra assimétrica aumentou, devido à

ção de uma estratégica eficaz de cibersegurança. Por outro lado, a própria doutrina nacional deverá ser desenvolvida em conjugação com entidades públicas e privadas." SILVA – ***Op cit.*** p. 41.

[1038] Ao que se associam os princípios de abertura, interoperabilidade, segurança e fiabilidade. *Ibidem*.

[1039] SILVA – ***Op cit.*** p. 41.

[1040] NUNES, Paulo – **Novos Desafios da Segurança e Defesa no Ciberespaço.** Conferência PGEES, 2012.

[1041] MILITÃO – ***Op cit.*** p. 39.

[1042] MILITÃO – ***Op cit.*** p. 40.

[1043] "O grande perigo da ciberguerra é que as ações tomadas no ciberespaço, vão expandir-se e perpetuar-se para fora dele, onde as suas consequências tendem a ser consequentemente mais graves e desastrosas do que se perspetivaria." *Ibidem*.

[1044] *Ibidem*.

[1045] Guerra entendida com uma ação recíproca violenta entre dois grupos políticos organizados (governos ou não). HUNTINGTON, Samuel – **A luta de guerrilhas. Antologia da Guerra Subversiva**. 1ª Parte, 1996. *apud* LARA, António – **Ciência Política - Estudo da Ordem e da Subversão.** 6ª Ed. Lisboa: Instituto Superior de Ciências Sociais e Políticas, 2011. p. 315.

[1046] PIGNATELLI, Marina – **Os Conflitos Étnicos e Interculturais.** Lisboa: Instituto Superior de Ciências Sociais e Políticas, 2010.

grande discrepância e sofisticação das ameaças, bem como o aumento dos fluxos migratórios e o ressurgir de ideologias extremas"[1047].

Como tal, verificamos a necessidade de coordenar a resposta da aplicação da lei europeia ao cibercrime, devido à natureza do crime organizado ter mudado radicalmente. Deste modo, o "uso de novas tecnologias por grupos do crime organizado não apenas alterou o *modus operandi* das formas tradicionais de crime, como também resultou no surgimento de todo um novo conjunto de crimes ciberdependentes"[1048].

Noutro patamar de atuação, a Guarda Nacional Republicana definiu a necessidade de "guiar-se pela premissa da constante abertura à mudança e uma constante capacidade de adaptação, ciente de que tanto em termos de estrutura da instituição, como em termos operacionais, a ideia de transformação deve ser uma constante"[1049], no sentido de "fazer face à complexidade do atual ambiente de segurança e às exigências de índole social, económica e informacional do mundo contemporâneo"[1050].

3.3.2. A Ciberguerra e os Princípios da Guerra Clássicos

O conceito de segurança abrange múltiplas construções[1051].

Genericamente, podemos afirmar que "este conceito que significa um estado de despreocupação, derivado do latim *securitas*, refere-se à qualidade daquilo que é seguro, ou seja, aquilo que está ao abrigo de quaisquer perigos, danos ou riscos"[1052].

Este conceito foi alargando o seu campo de ação, em especial, a partir da "década de 90 e passou a abranger, para além do militar, os campos político, económico, social, ambiental e de direitos humanos"[1053].

[1047] NYE, Joseph – **O Futuro do Poder.** Lisboa: Círculo de Leitores, 2012. e MILITÃO – ***Op cit.*** p. 41.
[1048] A Europol é a agência de aplicação da lei da UE, auxiliando os EM na luta contra graves crimes internacionais e terrorismo. Fundada como uma organização intergovernamental em 1999, é uma agência da UE desde 2010, tornando-a responsável perante o Conselho Justiça e Assuntos Internos (JAI) e o PE. A Europol não é uma força policial europeia e não possui poderes executivos. A Europol "fornece coordenação e apoio às agências policiais dos EM da UE. Todos os EM da UE têm agentes de ligação destacados para a sede da Europol em Haia, onde os agentes da polícia partilham informações entre si e com os analistas da Europol". Tradução livre do autor. BOLLE, Catherine de; BROUWER, Jelmer; MEULEN, Nicole van der – Coordenar a resposta da aplicação da lei europeia ao cibercrime. In DEFENCE – ***Op cit.*** p. 100.
[1049] Exemplo da importância desta mentalidade é a OTAN que criou o *Alied Comand of Transformation* para poder responder a este tipo de necessidades, sendo que a palavra-chave é transformação. QUADRADO, António – **A Estratégia de Segurança Interna da UE: o contributo da Guarda Nacional Republicana.** Lisboa: Instituto de Estudos Superiores Militares, 2015. Trabalho de Investigação Individual do CEMC – 2014/15. p. 28.
[1050] *Ibidem*.
[1051] RIBEIRO, António Silva – **Teoria Geral da Estratégia: O Essencial ao Processo Estratégico.** Coimbra: Edições Almedina, 2009.
[1052] MILITÃO – ***Op cit.*** p. 12.

Deste modo, importa fazer a distinção clássica entre o que é "a Segurança Interna e Segurança Externa, sendo a última um tema virado para o conceito de DN que tende a estar vinculada às FA e ao armamento, sendo estas o seu instrumento militar exclusivo"[1054].

Em complemento, refira-se que a "Segurança Nacional é a condição da Nação que se exprime na permanente garantia da sua sobrevivência em paz e liberdade, assegurando a soberania, independência e unidade, a integridade do território, a salvaguarda coletiva da população e bens inerentes e dos valores espirituais, o desenvolvimento normal das tarefas do Estado, a liberdade de ação política dos órgãos de soberania e o pleno funcionamento das instituições democráticas"[1055].

Já à Defesa Nacional está enquadrada e é definida como "o conjunto de medidas tanto de carácter militar como político, económico, social e cultural que, devidamente coordenadas, integradas e desenvolvidas tanto de uma perspetiva macro como sectorial, levam ao reforço direto das potencialidades de uma Nação. Minimizar as suas vulnerabilidades, com vista a torná-la apta a enfrentar todos os tipos de ameaça, direta ou indiretamente, que coloquem em causa a Segurança Nacional será o grande mote. Poderá ser entendida enquanto estrutura funcional que concorre para a consecução da segurança nacional como fim de Estado ou enquanto atividade instrumental de segurança externa da organização Estatal"[1056].

Outra distinção a fazer é a que se refere aos conceitos de cibersegurança e ciberdefesa. Assim, os "conceitos de cibersegurança e ciberdefesa são consideravelmente diferentes e cada um deles comporta uma esfera específica de ação no ciberespaço. A cibersegurança contém a ação das forças policiais e ainda dos serviços informáticos, a par que a ciberdefesa decorre exclusivamente das FA"[1057].

Deste modo, a cibersegurança deverá ser garantida por: FS (cibercrime e hacktivismo); e Serviços Informáticos (ciberespionagem e ciberterrorismo). Já a ciberdefesa deverá ser assegurada pelas FA, as quais deverão igualmente ter a capacidade de conduzir a ciberguerra.[1058]

[1053] Deste modo, "as medidas que visam a segurança são de largo espectro, envolvendo, também, a proteção civil, a segurança pública, as políticas económicas, de saúde, educativas, ambientais e as de garantia das instituições democráticas e da legalidade". MILITÃO – ***Op cit.*** p. 13.
[1054] *Ibidem*.
[1055] MILITÃO – ***Op cit.*** p. 14.
[1056] *Ibidem*.
[1057] MILITÃO – ***Op cit.*** p. 25.
[1058] Cfr. NUNES, Paulo – Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço. In **IV Simpósio sobre Segurança Informática e Cibercrime.** SimSIC: Beja, 2013. e BARBOSA – ***Op cit.*** p. 25.

A ciberguerra pode ser definida como "uma luta ou conflito entre duas ou mais nações ou entre diferentes fações dentro de uma nação onde o ciberespaço é o campo de batalha"[1059]. Consiste, deste modo, na materialização de ações de defesa ou de ataque contra todo o género de estruturas e redes de computador, sendo o campo de batalha conduzido numa dimensão digital.

De forma mais genérica, podemos definir ciberguerra como "qualquer ataque ou represália, intrusão ilícita nas redes ou computadores, assim como atos de espionagem, que ocorrem por meios informáticos e podem ser protagonizados por Estados ou Governos, ou por atores supra ou infra estatais. Estes atos por sua vez poderão estar ligados (ou não) a conflitos políticos ou militares no mundo real, ocorrendo em paralelo com uma conflitualidade física ou de forma totalmente autónoma"[1060].

Por outro lado, verifica-se uma enorme dependência dos "sistemas informáticos nos governos, empresas e organizações civis, onde em muitos casos e principalmente nos países em desenvolvimento existe a falta de recursos e mão-de-obra qualificada, os computadores normalmente estão equipados de *software* "pirata", que por sua vez os seus utilizadores são pessoas com pouca experiência ao invés de contratarem especialistas na área"[1061]. Nesta perspetiva, "os cyber-espiões encontraram uma vantagem enorme para conduzir as suas acções de exploração e ataques a redes de computadores (CNE e CNA), decorrente das vulnerabilidades encontradas"[1062].

Neste contexto, e com as Nações progressivamente mais dependentes do ciberespaço, onde "a informação está interligada digitalmente, onde cada vez mais empresas optam pelo uso da internet como meio principal de comunicação, emerge um possível e novo tipo de guerra a qual designamos de ciberguerra, onde a aquisição e a gestão de informação é uma das suas principais caraterísticas, sendo crucial proteger as IC das ameaças que surgem no ciberespaço"[1063].

Já na ótica do General Loureiro dos Santos, as operações de ciberguerra "podem ser executadas isoladamente de quaisquer outras, para obterem objectivos próprios, paralisan-

[1059] INSTITUTO DA DEFESA NACIONAL – **Op cit.** 2013.
[1060] MARTINS, M. – Ciberespaço: uma Nova Realidade para a Segurança Internacional. In **Nação e Defesa.** Lisboa: Instituto da Defesa Nacional, 2012. p. 133. e BARBOSA– ***Op cit.*** p. 11.
[1061] PERES – ***Op cit.*** p. 21.
[1062] ROHOZINSKI, Rafal – **Tracking GhostNet: Investigating a Cyber Espionage Network.** Toronto: University of Toronto, 2009.
[1063] PERES – ***Op cit.*** p. 24.

do ou destruindo redes de apoio de sistemas de vida e/ou sistemas de combates dos adversários"[1064].

O conceito de ciberguerra pode igualmente ser definido de acordo com as seguintes definições que se apresentam seguidamente:

- Na quinquagésima quinta sessão plenária da Assembleia Europeia de Segurança e de Defesa, realizada entre 2 e 4 de Dezembro de 2008, uma definição de ciberguerra foi apresentada por Christopher Chope e Tarmo Kõuts, como uma guerra com "recurso a computadores e internet para levar a cabo uma guerra no ciberespaço[1065].

- No dicionário de referência em França, a ciberguerra é toda a "agressão electrónica contra os sistemas informáticos perpetrados com o objectivo de utilizar como meio de propaganda e de desinformação ou de paralisar as actividades vitais de um País"[1066].

- De acordo com Laurent Murawiec[1067], ex consultor do Ministério de Defesa em França e especialista em assuntos militares e guerra da informação, a ciberguerra é o "conjunto de actividades de ordem e importância militar que têm lugar no seio desta nova dimensão", o ciberespaço.

- Por último, apresenta-se uma definição de ciberguerra do General Loureiro dos Santos que a considera como sendo "o conjunto de ações que é possível fazer no Ciberespaço, para obrigar um actor político a agir da forma que o actor que desencadeia essas acções pretende que haja"[1068].

Resumidamente, a ciberguerra poderá ser definida como o "ato de guerra entre grupos políticos, no ciberespaço, destinado a submeter o adversário à sua vontade, visando determinado fim político"[1069].

Recordemos igualmente uma definição para os designados ataques denegação de serviços (*DDoS*), os quais podem ser os ataques que visam "bloquear ou esgotar os recursos disponíveis de uma máquina impedindo que os outros lhe acedam"[1070].

[1064] "Mas também podem ser conduzidas em coordenação ou em apoio de ações noutros domínios, por exemplo com operações militares, como aconteceu durante a crise russo-estoniana de Maio de 2007 (tensão provocada pela deslocação do monumento ao soldado soviético, de uma praça pública para o cemitério) e na guerra dos cinco dias entre a Rússia e a Geórgia de Agosto de 2008". SANTOS – ***Op cit.*** 2009.

[1065] A igualmente denominada guerra cibernética. CHOPE – ***Op cit.*** p. 28.

[1066] ROBERT, Petit – **Le nouveau Petit Robert de la Langue Française.** 2010. [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://pr2010.bvdep.com/version-1/pr1.asp.

[1067] MURAWIEC, Laurent – La cyberguerre. In **AGIR - Revue Génerale de Stretégie. Révolution de l'information, crise de Communication.** N.º 2. 1999.p. 3.

[1068] PERES – ***Op cit.*** p. 24.

[1069] PERES – ***Op cit.*** p. 8.

[1070] SANTOS, José – **As Guerras que já aí estão e as que nos esperam - se os políticos não mudarem.** Mem Martins: Publicações Europa-América, 2009. p. 169.

Para análise dos Princípios da Guerra Clássicos, no que respeita às "doutrinas de ciberguerra", iremos considerar as seguintes referências[1071]:

- No que concerne à delimitação e definição de Ciberespaço o manual de doutrina dos EUA "*Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*"[1072], o dicionário de termos militares dos EUA "*Department of Defense Dictionary of Military and Associated Terms*"[1073], a política para o ciberespaço da Casa Branca "*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*"[1074], a estratégia de cibersegurança do Reino Unido "*Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space*"[1075], o Livro Branco de Defesa e Segurança Nacional da França[1076], o livro "As Guerras que já aí estão e as que nos esperam – se os políticos não mudarem" do General Loureiro dos Santos[1077], e o Livro Verde relativo a um Programa Europeu de Proteção das IC[1078];
- Já em relação à delimitação e definição de ciberguerra, tem-se como referências a 55.ª sessão da Assembleia Europeia de Segurança e de Defesa[1079], e um trabalho ("*La Cyberguerre*") realizado por um ex-consultor do Ministério de Defesa em França, especialista em assuntos militares e guerra da informação Laurent Murawiec[1080];
- Outras referências utilizadas são a doutrina de segurança da informação da Federação Russa, onde está explícito oficialmente a totalidade das metas, objectivos, princípios e diretrizes básicas para garantir a segurança da informação na Federação Russa[1081], relatórios de

[1071] PERES – ***Op cit.*** p. 8-9.
[1072] JP 2-01.3. – **Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace.** 2000.
[1073] JP 1-02. – **Department of Defense Dictionary of Military and Associated Terms.** 2009.
[1074] CASA BRANCA – **Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.** Washington: [s.n.], 2009.
[1075] OCS – **Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space**. Norwich: TSO, 2009.
[1076] LE LIVRE BANC – **Défense et Sécurité nationale.** Paris: Odile Jacob, 2008.
[1077] SANTOS – ***Op cit***. 2009.
[1078] COMISSÃO EUROPEIA - **Livro Verde: Relativo a um programa Europeu de protecção das infraestruturas críticas.** Bruxelas: s.n., 2005. COM(2005) 576 final.
[1079] CHOPE, M. Christopher; KÕUTS, M. Tarmo – **CINQUANTE-CINQUIÈME SESSION - La guerre informatique.** 2008.
[1080] MURAWIEC – ***Op cit.***
[1081] DISRF – **Doctrine of the Information Security of the Russian Federation.** 2000. [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.medialaw.ru/e_pages/laws/project/d2-4.htm.

Wilson Clay que abordam a temática dos ciberataques[1082], um relatório de Bryan Krekel sobre as capacidades da República Popular da China para conduzir ciberguerra e CNE[1083].

No que respeita à doutrina do Exército dos EUA são nove os "Princípios da Guerra adotados: Objetivo, Ofensiva, Massa, Economia de Forças, Manobra, Unidade de Comando, Segurança, Surpresa, Simplicidade"[1084]. De igual modo, em Portugal, na doutrina militar nacional são adotados os mesmos Princípios da Guerra dos EUA, a saber: Objetivo, Ofensiva, Massa, Economia de Forças, Manobra, Unidade de Comando, Segurança, Surpresa, Simplicidade. Estes serão os princípios para os quais se procurará verificar a sua aplicabilidade em relação às novas tipologias de guerra, designadamente às operações de ciberguerra desenvolvidas num novo domínio designado de ciberespaço.[1085]

Tabela 1 – Princípios da Guerra Clássica e respetivos indicadores[1086]

[1082] CLAY, Wilson – **Cyberwarfare.** Washington DC: CRS Report for Congress, 2001. RL30735. e CLAY, Wilson – **Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues.** Washington DC: CRS Report for Congress, 2007. RL31787.
[1083] KREKEL, Bryan – **Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.** McLean: Northrop Grumman, 2009.
[1084] PERES – ***Op cit.*** p. 14.
[1085] PERES – ***Op cit.*** p. 17.
[1086] PERES – ***Op cit.*** p. 18-19.

Princípios da Guerra (RC 130-1)	INDICADORES	
	Definição	**Palavras-Chave**
Objectivo	- Qualquer operação militar deverá contribuir para obtenção do **objectivo último** da guerra (aniquilamento das forças armadas do adversário e da sua vontade de combater);	Objectivo último
	- **Objectivos definidos de forma clara** e inequívoca;	Objectivos claros
	- Devem ser **exequíveis** e alcançados com os meios que a força dispõe;	Objectivos exequíveis
	- Objectivos escolhidos **em função da missão**, dos **meios disponíveis**, do **inimigo** e das **características da área de operações**.	
Ofensiva	- Acção Ofensiva necessária para **obter resultados decisivos** e para conservar ou reconquistar a liberdade de acção;	Resultados decisivos
	- Acção Ofensiva permite tomar iniciativa, impor a sua vontade ao inimigo, marcar o ritmo e influenciar o curso da batalha e explorar os **pontos fracos do inimigo**.	Pontos fracos do IN
Massa	- **Empregar potencial de combate superior** ao inimigo no local e momento decisivo;	Potencial superior
	- Este princípio em conjugação com os outros princípios permite a forças numericamente inferiores no seu conjunto, obtenham uma superioridade local e momentânea, decisiva para o desenrolar das operações.	
Economia de Forças	- **Emprego judicioso dos meios** à sua disposição, reduzindo ao mínimo o desgaste desses meios e procurando empregá-los de forma decisiva no local e momento mais adequados;	Emprego judicioso dos meios
Manobra	- **Dispor as forças** de forma a colocar o Inimigo em posição desvantajosa;	Disposição das forças
	- Permite a correcta aplicação do princípio da massa e o **princípio da economia de forças**;	Massa e Economia de Forças
	- Contribui para **conservar liberdade de acção**, manter **iniciativa** e **explorar os resultados do combate.**	Liberdade de acção Iniciativa
Unidade de Comando	- **Acção coordenada** de todas as forças de forma a fazer convergir os seus esforços tendo em vista um objectivo comum;	Acção coordenada
	- Existência de Unidade de **Doutrina e de Comando** a orientarem a acção das forças;	Unidade de Doutrina e Comando
	- **Investir num único Comandante a autoridade necessária**.	Autoridade única
Segurança	- Permite **conservar liberdade de acção**;	Liberdade de acção
	- **Permite negar ao Inimigo a possibilidade de obter informações sobre as forças amigas e os seus planos** e evita-se ser surpreendido pelo adversário;	Informação
Surpresa	- **Criar situações inesperadas** para o qual o Inimigo não esteja em condições de reagir eficazmente em tempo oportuno;	Situações inesperadas
	- Permite retirar ou **limitar liberdade de acção do adversário**, colocando-o em posição desvantajosa;	Posição desvantajosa
	- Contribui para a surpresa a velocidade, a decepção, a concentração inesperada de forças num dado local e momento;	Manobra Ofensiva Segurança
	- A surpresa **facilita a manobra**, estimula a **ofensiva** e favorece a **segurança**.	
Simplicidade	- **Planos simples** e os objectivos e as ordens claras e concisas.	Plano simples

Com efeito, os nove Princípios da Guerra apresentados na Tabela 1, bem como os respetivos indicadores, terão a finalidade de orientar a análise relativa à possibilidade de justificar a "utilização na ciberguerra dos diversos Princípios da Guerra referidos"[1087].

Mais à frente, iremos procurar demonstrar a possibilidade da existência de operações de ciberguerra associadas a um novo domínio do ciberespaço, tendo em vista *a posteriori*

[1087] PERES – ***Op cit.*** p. 18.

analisar se realmente os Princípios da Guerra fixados anteriormente como referencial também podem ser aplicados à ciberguerra.[1088]

Em complemento, refira-se ainda que cada vez mais é necessário "obter uma capacidade tecnológica no domínio da segurança, pelo que, uma superioridade nesta área, poderá ser decisivo para o sucesso de qualquer campanha militar, exigindo estruturas próprias de ciberdefesa e cibersegurança, capazes de deter os ataques de adversários e levar a cabo ataques cibernéticos preventivos como manobras de antecipação e/ou resposta num conflito armado ou não"[1089].

Acompanhando esta linha de pensamento, os EUA procuraram uma solução, pelo que, a ciberguerra no âmbito da doutrina americana "pode ser conduzida contra qualquer um dos meios que tenha acesso ao ciberespaço, podendo incluir *hardware*, redes, *software*, dados, procedimentos e operadoras que fornecem acesso à internet, visto existir relativa vulnerabilidade[1090] em cada um desses componentes"[1091].

Em complemento, após os ataques que os EUA foram alvo, a crescente preocupação dos mesmos conduziu à criação em 2007 de um *Cyber Command*, atribuindo como missão à U. S. Air Force: "voar e lutar no ar, no espaço e ciberespaço"[1092]. A "criação deste *Cyber Command* e a atribuição de uma nova missão, revela o surgimento de uma nova forma de fazer a guerra (a ciberguerra), e a existência de uma preocupação por parte dos EUA com a defesa e o controlo do ciberespaço"[1093].

No seguimento, no dia 23 de junho de 2009 foi criado uma componente de ciberdefesa dentro do Comando Estratégico dos EUA (USSTRATCOM), o *Cyber Command* dos EUA (USCYBERCOM). Este *Cyber Command* entrou em atividade a 21 de maio de 2010, tendo como missão planear, coordenar, sincronizar e conduzir operações de defesa das redes de informação do departamento de defesa e preparar para, quando solicitado conduzir operações no Ciberespaço a fim de permitir ações em todos os domínios, certificando-se

---

[1088] PERES – ***Op cit.*** p. 19.
[1089] É com esta preocupação que os diversos Estados e Organizações Internacionais têm investido nesta área, onde iremos referir algumas das medidas tomadas por parte delas, com o objectivo de tornar claro que, nos dias de hoje, Estados e Organizações Internacionais (e.g. E.U.A., Rússia, China, França e OTAN) têm manifestado preocupação quanto à possibilidade de ocorrerem Ciberguerras no novo domínio que atrás designámos de Ciberespaço. SANTOS – ***Op cit.*** 2009. p. 303.
[1090] Essa vulnerabilidade existe por várias razões, como por exemplo a falta de treino adequado do utilizador, más instalações físicas combinado ainda com o nível de sofisticação do inimigo para levar a cabo ataques a redes de computadores (CNA).
[1091] PERES – ***Op cit.*** p. 25.
[1092] CLAY, Wilson – **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.** Washington DC: CRS Report for Congress, 2008. p. 7.
[1093] *Ibidem*.

que os EUA e seus aliados consigam ter liberdade de ação no ciberespaço e negar o mesmo aos adversários[1094].

Para os EUA, as ações militares no Ciberespaço englobam as CNO, nas quais as "ações militares desenvolvidas são principalmente assegurar a proteção das suas infraestruturas críticas, redes e defenderem-se de possíveis ataques maliciosos a partir da internet, [sendo] todas as ações que se podem desenvolver no espectro electromagnético"[1095].

Por outro lado, vejamos agora a solução apresentada pela OTAN.

A OTAN encontra-se há muito tempo já familiarizada com "a defesa contra a guerra da informação e a guerra electrónica, desenvolvendo esforços significativos para conduzir operações de guerra centrada em rede e respetivas capacidades em rede, sendo que, em 2002, na cimeira de Praga, dirigentes da OTAN decidiram reforçar as defesas contra ataques cibernéticos, o que resultou num conjunto de decisões, das quais se salienta o programa de ciberdefesa, envolvendo vários órgãos"[1096].

Após os acontecimentos de 2007 na Estónia, a OTAN decidiu "acelerar o desenvolvimento do centro de excelência de ciberdefesa do ciberespaço[1097] que ficaria situado na capital da Estónia (Tallinn), estabelecido formalmente a 14 de maio de 2008, a fim de aumentar a capacidade de defesa da OTAN, (…) sendo que a missão atribuída a este centro de excelência é de aumentar a capacidade de cooperação e partilha de informação dentro da OTAN, entre as nações pertencentes à OTAN e parceiros em ciberdefesa, por força da educação, investigação e desenvolvimento, lições aprendidas e consulta"[1098].

Decorrida que está esta análise contextual e ideológica, passamos agora para a análise dos Princípios da Guerra Clássica à luz do estudo de caso da Estónia, a saber:

1) Princípio do Objetivo – Admitindo a possibilidade de existirem operações militares no ciberespaço, as mesmas deverão contribuir para a "obtenção do objetivo último da guerra que é o aniquilamento das FA do adversário e da sua vontade de combater". Todavia, "os

---

[1094] ALEXANDER, Keith B. – **United States Strategic Command.** 2010. [Em Linha]. [Consult. 25 Jun. 2018]. Disponível em WWW:<URL: http://www.stratcom.mil/factsheets/cc/.

[1095] PERES – ***Op cit.*** p. 26.

[1096] OTAN *Communication and Information Systems Services Agency*, OTAN *Information Security Technical Centre*, OTAN *Information Security Operations Centre* e OTAN *Computer Incident Response Capability*. CORNISH, Paul – **Cyber-Security and Politically, Socially and Religiously.** Brussels: European Parliament, 2009. PE 406.997. e PERES – ***Op cit.*** p. 29.

[1097] A CCDCOE está a desenvolver-se desde 2004, a qual se denomina de *Cooperative Cyber Defence Centre of Excellence*. A CCDCOE contou com sete Nações patrocinadoras (Estónia, Alemanha, Itália, Letónia, Lituânia, Eslováquia e Espanha), sendo que em novembro de 2008 os EUA aceitaram fazer parte desta organização. CORNISH – ***Op cit.***

[1098] Este centro de excelência recebeu acreditação plena da OTAN a 28 de Outubro de 2008, alcançando o *status* de Organização Militar Internacional. Cfr. CCDCOE [Consult. 03 Jan. 2018]. Disponível em WWW:<URL: http://www.ccdcoe.org.

objetivos traçados numa operação de ciberguerra serão forçosamente diferentes dos objetivos traçados numa operação terrestre, área, marítima, por via dos meios utilizados e das respectivas caraterísticas da área de operações". No caso dos ataques cibernéticos dirigidos contra a Estónia podemos constatar que os objetivos foram as IC da internet com o objetivo de "bloquear sítios oficiais como por exemplo do Primeiro-Ministro, Parlamento, da Presidência da República, destabilizar as operações dos maiores bancos da Estónia, serviços de saúde e tecnologia, e afectaram os sítios de vários jornais diários".[1099]

2) Princípio da Ofensiva – Este princípio da guerra é aplicável no caso da Estónia, uma vez que se verificou o lançamento de uma ofensiva cibernética contra as IC da internet, na perspetiva de este Estado ter tido dificuldade em recuperar (os ataques duraram semanas, ao invés de horas ou dias), "sendo que foram explorados com sucesso os pontos fracos da Estónia (grande dependência da Estónia em relação às tecnologias da informação), remetendo a Estónia a uma posição defensiva, na medida em que a OTAN e os EUA enviaram peritos na área da segurança para ajudar a Estónia a recuperar dos ataques, analisar os métodos utilizados pelo inimigo e tentar determinar as fontes dos ataques"[1100].

3) Princípio da Massa – Este princípio foi verificado na capacidade de lançamento de ataques de negação de serviço (*DDoS*), tendo conseguido destabilizar o normal desenrolar das operações, como por exemplo, as operações dos maiores bancos da Estónia via internet. Os referidos ataques normalmente têm "início a partir de um computador[1101] que tem sob seu comando milhares de outros computadores infectados espalhados por todo o Mundo (denominados de computadores "*zombies*") que são preparados para lançarem ataques à ordem do computador "Mestre" contra um determinado recurso de um servidor com o objectivo deste não conseguir dar resposta a todos os pedidos, obrigando o servidor a reiniciar ou mesmo a ficar indisponível durante algum tempo"[1102].

4) Princípio da Economia de Forças – No caso da Estónia, este princípio da guerra não é fácil tirar conclusões precisas, considerando não existir informação suficiente para se saber se "os ataques foram resultado de raiva espontânea de atacantes com o objectivo de se mostrarem indignados com a mudança da estátua para o cemitério militar, ou se foi algo coordenado e incentivado pelo Governo Russo. Ou seja, das informações que dispomos

[1099] PERES – ***Op cit.*** p. 35.
[1100] *Ibidem*.
[1101] Denominado de computador "Master" (Mestre).
[1102] PERES – ***Op cit.*** p. 35.

podemos concluir que não houve qualquer planeamento com vista ao emprego judicioso dos meios (conjunto de *botnets*) em locais e momentos adequados"[1103].

5) Princípio da Manobra – Este "princípio da guerra verifica-se, pois quando se pretende dispor uma força de forma tal que o inimigo fique colocado numa situação desvantajosa, no caso da ciberguerra e neste estudo de caso da Estónia, podemos facilmente verificar que através dos milhares de computadores infectados espalhados pelo mundo (rede de *botnets*), conseguiu-se com sucesso saturar os servidores das IC da internet da Estónia e contribuindo para conservar a liberdade de ação, para manter a iniciativa e explorar os resultados do combate[1104]"[1105].

6) Princípio da Unidade de Comando – Os dados existentes não nos permitem saber se este princípio da guerra foi aplicado no caso da Estónia. Todavia, "no nosso ponto de vista, este é um princípio da guerra que se revela pouco importante na ciberguerra, [apesar de] acharmos necessário o desenvolvimento de ferramentas importantes, como por exemplo, no caso da OTAN, com o desenvolvimento do seu ciber-comando e de plataformas inteletuais, doutrinárias e estratégicas, (…) de forma a coordenar operações de ciberguerra"[1106].

7) Princípio da Segurança – Este princípio da guerra verificou-se neste caso de ciberguerra da Estónia, uma vez que "apenas conseguiram condenar uma pessoa. Os autores destes ataques conseguiram garantir o seu anonimato impossibilitando a Estónia de obter informações precisas dos autores da origem dos ataques. Este princípio da guerra foi necessário para o sucesso de todos os outros princípios na medida em que para se alcançar por exemplo o princípio da liberdade de ação, conseguiu-se negar ao inimigo a possibilidade dele obter informações sobre os ataques que estavam planeados, alcançando os objectivos pretendidos, ocultando informações sobre si próprios"[1107].

8) Princípio da Surpresa – Este foi um dos principais princípios da guerra, considerando que "os ataques dirigidos contra a Estónia foram efectuados de tal forma que [a mesma] não estava preparada para responder de forma eficaz, colocando-a em posição desvantajosa na medida em que a incerteza de não conhecer o iniciador destes ataques afecta também a decisão de decidir quem será alvo de retaliação"[1108].

[1103] PERES – ***Op cit.*** p. 36.
[1104] Paralisando a economia da Estónia e impedir que a disseminação de informação se fizesse para o exterior.
[1105] PERES – ***Op cit.*** p. 36.
[1106] *Ibidem*.
[1107] *Ibidem*.
[1108] PERES – ***Op cit.*** p. 37.

9) Princípio da Simplicidade – A simplicidade foi conseguida através da utilização de *bot-nets*[1109], assumindo-se assim como uma "ferramenta importante para levar a cabo este tipo de operações no ciberespaço, porque podem ser facilmente concebidos e de forma eficaz para interromper sistemas de computadores de diferentes formas, e porque um utilizador mal-intencionado, sem possuir grandes capacidades técnicas, pode dar início a esses efeitos negativos no ciberespaço, contribuindo para a eficácia e o sucesso das operações"[1110].

Com efeito, poderemos sumarizar as seguintes conclusões deste subcapítulo:

- No caso dos ciberataques na Estónia verificámos que a maioria dos "Princípios da Guerra se revelaram importantes para uma ação de ciberguerra, à exceção do princípio da economia de forças e do princípio da unidade de comando"[1111].

- A origem dos ataques na Estónia não é suficientemente esclarecedora, não obstante existirem suspeitas de que a execução dos mesmos poderá ser assacada à Rússia[1112].

- O princípio do objectivo, princípio da ofensiva, princípio da massa, princípio da manobra, princípio da segurança, princípio da surpresa e o princípio da simplicidade são todos importantes para uma ação de ciberguerra no ciberespaço, sendo as exceções o princípio da economia de forças e o princípio da unidade de comando[1113]. Todavia, o princípio da unidade de comando poderá vir a revelar-se importante, por exemplo, com "a criação de centros de ciberdefesa (por exemplo, a criação do "*Cyber Command*" nos EUA e do Ciber-Comando para a Cibersegurança na OTAN, em Bruxelas), onde será exigido certamente o princípio da unidade de comando, de forma a fazer convergir todos os esforços tendo em vista um objectivo comum. Contudo, deverá ter-se em conta que este princípio poderá ser quebrado com o uso de comunidades de *hackers* (hacktivistas) em apoio das operações de ciberguerra. Ou seja, o princípio da unidade de comando poderá ser repartido por vários pontos de decisão"[1114].

- A ciberguerra implica a obtenção de uma capacidade tecnológica no domínio da segurança, exigindo estruturas próprias de ciberdefesa e cibersegurança, com vista a antecipar ata-

[1109] Refere-se ao conjunto de computadores infectados com códigos maliciosos, designados de computadores "*zombies*" e controlados remotamente através de comandos enviados através da internet.
[1110] Suspeita-se que estes ataques foram planeados e disponibilizados na internet para qualquer cidadão que entendesse entrar nesse movimento de revolta e atacar as IC da internet da Estónia. PERES – ***Op cit.*** p. 37.
[1111] *Ibidem*.
[1112] *Ibidem*.
[1113] *Ibidem*.
[1114] PERES – ***Op cit.*** p. 44.

ques desta natureza, ou mesmo e perpetrar ataques cibernéticos num conflito armado em coordenação ou não com outros teatros de operações.[1115]

- Os "Princípios da Guerra continuam atuais e relevantes para ações de ciberguerra e podem ser aplicáveis e usados na ação de comando e controlo dos chefes militares"[1116].

- O princípio do objetivo é aplicável na ciberguerra "na medida em que é possível traçar objetivos claros e exequíveis em função da missão e meios colocados à disposição tendo em conta as caraterísticas da área de operações que é o ciberespaço"[1117].

- O "princípio da ofensiva continua a ser um princípio importante porque é possível lançar ofensivas neste novo espaço operacional procurando explorar os pontos fracos das tecnologias de informação em complemento ou não de ações desenvolvidas noutros teatros de operações para alcançar resultados decisivos"[1118].

- O "princípio da massa pode ser alcançável e verifica-se na ciberguerra, porque é possível com os meios existentes e vulnerabilidades decorrentes das tecnologias de informação obter a determinado momento em local e momento decisivo potencial de combate superior, por exemplo, com o uso dos milhares de computadores ligados à internet espalhados pelo mundo"[1119].

- O princípio da economia de forças é um dos dois princípios que "não foi possível tirar conclusões, contudo temos a perceção de que é um princípio que não deixa de ser importante porque se a ciberguerra é algo estritamente de cariz militar, e por consequência em todas as ações militares é exigido o emprego judicioso dos meios, este é um princípio que não pode ser posto de parte, exigindo um controlo dos meios à sua disposição"[1120].

- O "princípio da manobra também se revelou importante para a ciberguerra porque é possível dispor as forças (não fisicamente, mas virtualmente como por exemplo empregar computadores infetados de todos os cantos do mundo) e colocar o adversário em posição desvantajosa"[1121].

- O "princípio da unidade de comando à semelhança do princípio da economia de forças não se revelou tanto até ao momento, também pelo motivo de o virtual ser ainda um espaço onde qualquer um pode ter a iniciativa e levar a cabo ações ilícitas (por exemplo, *hackers*

[1115] PERES – ***Op cit.*** p. 47.
[1116] *Ibidem*.
[1117] *Ibidem*.
[1118] *Ibidem*.
[1119] *Ibidem*.
[1120] *Ibidem*.
[1121] PERES – ***Op cit.*** p. 48.

desenvolverem de forma autónoma ataques a redes), o que poderá colidir e comprometer as ações militares"[1122].

- O princípio da segurança é um princípio que pode ser atingido na ciberguerra, devido a ser "possível conservar a liberdade de ação ao negar a possibilidade do adversário obter informações dos nossos planos"[1123].

- O "princípio da surpresa está presente na ciberguerra porque é possível criar situações inesperadas atacando IC da internet e obter informações importantes"[1124].

- O "princípio da simplicidade é um dos princípios que facilmente é "alcançável na medida em que com os meios disponíveis é relativamente fácil e barato e está ao alcance de qualquer um elaborar planos simples e atacar IC da internet"[1125].

- As "ações de ciberguerra no ciberespaço podem ser planeadas tendo em consideração o princípio do objectivo, princípio da ofensiva, princípio da massa, princípio da manobra, princípio da segurança, princípio da surpresa e o princípio da simplicidade, de modo a orientar a ação de comando dos chefes militares, auxiliando-os num planeamento racional e eficiente nas suas operações de ciberguerra"[1126].

- Para concluir, podemos referir que "a ciberguerra constitui um novo método para desenvolver Operações Militares. Operações Militares de natureza, um pouco diferentes daquelas conhecidas até hoje, pelo facto de se desenvolverem num Teatro de Operações bastante diferente dos que se conhecem, designado por ciberespaço. Sendo que a ciberguerra, constitui hoje, um método aceite para desenvolver operações militares, que engloba um conjunto de ações (CNA, CND e CNA) que são desenvolvidas no ciberespaço, de modo a atingir determinado fim político"[1127].

3.4. O Uso da Força no Ciberespaço

O uso da força no ciberespaço é uma problemática pertinente e cada dia mais assume contornos de obrigatoriedade no que respeita ao planeamento e execução das ditas Operações Militares, considerando o desuso destas Operações nos moldes mais convencionais.

Antes de mais, tal como já estudámos, refira-se que o desenvolvimento de normas para a conduta dos Estados no ciberespaço não exige uma reinvenção do direito internacio-

[1122] *Ibidem*.
[1123] *Ibidem*.
[1124] *Ibidem*.
[1125] *Ibidem*.
[1126] *Ibidem*.
[1127] *Ibidem*.

nal consuetudinário, considerando que as normas internacionais já existentes que delimitam o comportamento dos Estados, em tempos de paz ou de conflito, também têm aplicação no ciberespaço.

Porém, a resposta a este tipo de eventos obriga a fomentar a cooperação internacional, não obstante a dificuldade e o desafio que constituem a necessidade de obtenção de um consenso nestas matérias do uso da força no ciberespaço, sem a qual, a resposta a este tipo de eventos não é eficaz. Tal, assenta na dificuldade de definição de regras jurídicas comuns que possibilitem aos Estados a aplicação de um direito sancionatório para os infratores e respetivos apoiantes, tal como acontece com o terrorismo.

De igual modo, o recurso a uma resposta militar dependerá da qualificação ou não do ciberincidente, no que concerne ao uso da força, pelo que, importa compreender em que casos se verificam o uso da força. Assim, considera-se que há uso da força quando um qualquer ciberincidente provoca estragos físicos ou danos corporais ou, no limite, a morte de pessoas. Com efeito, assinale-se que a licitude do recurso aos meios militares e ao uso da força apenas se afigura viável quando os ciberincidentes sejam imputáveis a outro Estado e sejam, eles próprios, qualificáveis como uso da força.

Em contraponto, verificamos que nos casos em que não há informações de mortes de pessoas ou danos corporais, deveremos explorar a hipótese de se considerar existir uso da força nas situações em que se verificam danos físicos motivados pela falta de eletricidade e comunicações. Nesta eventualidade, quando os ciberincidentes são imputáveis a um Estado, de acordo com os indícios recolhidos, e se constate o uso da força considera-se que há direito de legítima defesa, nos termos do art.º 51.º da CNU, por parte do Estado que é vítima dos ciberincidentes.

Assim, a legítima defesa pressupõe a existência de um ataque armado contra um determinado Estado. Com efeito, a determinação da existência de uma ameaça à paz, a rotura da paz ou ato de agressão nos termos do art.º 39.º da CNU, que as medidas provisórias e as sanções coativas não militares de acordo com os art.ºs 40.º e 41.º da CNU, respetivamente, não pudessem ser ou não se tenham revelado eficazes, são os fundamentos para aplicar as sanções coativas militares.

Deste modo, as sanções coativas militares ao abrigo do Capítulo VII (art.º 42.º da CNU) surgem como *ultima ratio*, sendo aplicáveis se o CS considerar que as medidas previstas no art.º 41.º da CNU seriam ou demonstraram ser inadequadas, concretamente, com a interrupção de relações económicas/diplomáticas ou a interrupção de meios de comunicação. Este art.º 42º da CNU encontra-se limitado pelo princípio da proporcionalidade.

Nestas condições, poderá existir um recurso legítimo ao uso da força, quer por parte do Estado agredido, quer por parte de um Estado terceiro (conceito de defesa coletiva). Todavia, mesmo no caso dos ciberincidentes, importa ainda realçar que este direito está vinculado ao princípio da proporcionalidade, isto é, a resposta à "agressão" terá que ser proporcional (sentido estrito), necessária (única hipótese possível) e adequada (os meios não devem ultrapassar os fins), a fim de se evitar o "excesso de legítima defesa".

No direito de legítima defesa registe-se que existem princípios a terem de ser respeitados pelo Estado, de acordo com o direito consuetudinário internacional, no sentido da possibilidade do recurso ao uso da força, a saber: o princípio da necessidade de atuação; o princípio da proporcionalidade na resposta; o princípio da adequação da resposta; e o princípio da atualidade da ameaça.

Neste particular, caso o Estado vítima pretenda fazer o uso da força, mesmo que seja numa situação de legítima defesa, de acordo com o art.º 51.º da CNU, terá de informar o CS das NU e equacionar pedir ajuda militar à OTAN, caso consiga identificar as forças estrangeiras responsáveis pelo ataque, a fim de solicitar eventual apoio técnico e, acima de tudo, informar os restantes EM quanto ao risco para a sua defesa, no sentido de se equacionar um uso conjunto das forças militares de EM da OTAN.

Em complemento, registe-se que o princípio da proibição do recurso à força encontra previsão na CNU, nos artigos 2.º e 3.º, bem como nas Resoluções 2625 e 3314, as quais correspondem respetivamente aos Casos Nicarágua e Iraque. Estas Resoluções permitem identificarmos os conceitos de: definição de agressão (uso ilegal da força contra a CNU); ameaça à integridade territorial; ameaça à independência política; princípio da adequação; princípio da proporcionalidade; e solução pacífica de conflitos (art.º 36.º da CNU).

Deste modo, importará num futuro próximo haver uma definição de alguns destes conceitos adaptados aos ciberincidentes, uma vez que existe uma dificuldade acrescida de, por exemplo, definir os conceitos de agressão, agressor, território e adequação dos meios.

Por outro lado, alguns autores consideram que atualmente o direito internacional sobre o uso da força cessou por desuso, devido à sua constante violação pelos Estados. Contudo, no caso dos ciberincidentes, este é um direito que cada vez mais se afigura como atual e pertinente, o qual urge positivar em normas internacionais, a fim de evitar abusos.

Todavia, já vimos que em 2005, na Cimeira Mundial de Chefes de Estado e de Governo dos EM das NU, foi reafirmado que as disposições da CNU são suficientes para responder a todo o tipo de ameaças internacionais à paz e à segurança.

Logo, o fundamental não é questionar o *jus ad bellum* no pós II Guerra Mundial, mas clarificar o âmbito e os efeitos da proibição do uso da força enquanto regra fundamental para a prevenção de conflitos armados no século XXI, em particular à luz das transformações que o desenvolvimento tecnológico introduziu nos sistemas de defesa dos Estados e da emergência de novas ameaças securitárias, como o terrorismo transnacional ou a proliferação de armas de destruição maciça, a par dos ciberincidentes.

Neste sentido, o Direito Internacional deverá refletir e atribuir uma particular importância à regulamentação sobre o que se considera agressão, uma vez que da sua existência dependerá a legitimidade e a legalidade de uma resposta armada de um Estado ou grupo de Estados, a título de um direito inalienável dos mesmos a uma legítima defesa.

O ato de agressão, de acordo com o art.º 2.º da referida Resolução 3314 de 1974, para ser considerado como tal, tem como premissa o facto de ter o primeiro Estado utilizado da força armada em violação à CNU. Já em relação aos ciberincidentes, a questão principal passa, entre outros aspetos, por conseguir atribuir o referido ato a um Estado, uma vez que muitas vezes estamos a falar de atos perpetrados por atores individuais, Estados falhados ou até organizações terroristas, sendo que nesta área muitas vezes não se consegue atribuir a execução de um ato de forma indubitável, o que levanta posteriormente problemas na definição de agressão e no exercício da legítima defesa.

Por sua vez, o art.º 3.º vem escalpelizar alguns exemplos, de forma taxativa, de atos que se podem considerar como agressão. Atualmente, a questão será de perceber se estivermos a falar do caso de um ciberincidente ou ciberataque, se consideramos ou não como um ato de agressão. Numa primeira análise, estamos inclinados a concluir que um ciberataque se constituirá como uma agressão, desde que este se destine direta ou indiretamente a afetar a soberania, integridade territorial ou independência política de outro Estado.

Quanto ao conceito de ataque armado, e tendo por base as inúmeras evoluções tecnológicas no domínio do armamento, cada vez mais assume um caráter difuso e que se afasta dos conceitos clássicos. Assim, poderemos considerar como ataque armado qualquer operação ou ato com o efeito de infligir um prejuízo ou dano no Estado e nos seus elementos fundamentais, apesar da dificuldade de concretização prática nos ciberincidentes.

Recordemos igualmente que os efeitos da legítima defesa subsumem-se à aplicação do uso da força com o objetivo de repelir o ataque armado que está sendo perpetrado contra a respetiva vítima, de acordo com as caraterísticas da atualidade ou da iminência, bem como do uso proporcional dos meios, incluindo os casos de ciberincidentes.

Por outro lado, o direito de legítima defesa baseia-se na existência de um ataque armado perpetrado contra um Estado, o qual pode ser praticado pelo próprio Estado ou por Estados terceiros, tratando-se neste último caso de uma legítima defesa coletiva.

Noutro sentido, a doutrina maioritária tem alegado que a responsabilidade estadual não é imprescindivel para os efeitos do art.º 51º da CNU. Esta posição é sustentada com recurso às Resoluções 1368 e 1373, nas quais o CS qualificou os ataques terroristas de 11 de setembro de 2001 como um ataque armado, pelo que, se verifica a necessidade de se dissociar o direito de legítima defesa de uma responsabilidade estadual. No caso de um ciberataque essa necessidade aumenta de forma exponencial.

Em relação ao ataque armado para efeitos de legítima defesa, o que está em causa é ser um qualquer ataque armado, ao invés de se diferenciarem os seus autores ou as armas utilizadas para o efeito. Assim, as novas tiplogias de ataques possibilitam uma leitura ampliativa do art.º 51º, considerando que um ataque armado pode ser realizado de forma convencional ou não convencional, pelo que um ataque em rede pelo computador poderá ser considerado um ataque armado se tal agressão vier a causar uma qualquer fatalidade, como por exemplo, a inoperacionalização de sistemas computadorizados que controlam as redes de abastecimento de água e barragens, causando a inundação de regiões habitadas.

Quanto ao *jus ad bellum*, nos termos do capítulo VII, constatamos que deveria ser adotada uma resolução pelo CS que prescrevesse os princípios e critérios para o recurso ao uso da força, os quais seriam atualizados regularmente com base nas experiências reunidas, com lista de conflitos em curso anexada e definidores de uma ameaça à paz de acordo com o art.º 39º, devendo ser igualmente considerada a questão do uso da força no ciberespaço.

Neste contexto, o Manual de Tallinn teve o condão de ser o primeiro documento orientador que define a legitimidade para a ciberguerra, tendo por base os princípios das Leis internacionais, do respeito pela soberania dos Estados e da defesa dos Direitos Humanos. Quanto à proibição de ameaça ou uso da força, o mesmo defende que só poderá ser realizada uma operação cibernética quando estivermos perante uma ameaça ilegal ou o uso da força contra a integridade territorial ou independência política de qualquer Estado, bem como de qualquer outra maneira inconsistente com os propósitos das NU.

Deste modo, o recurso ao uso da força apenas se pode verificar quando todos os outros meios de alcançar um objetivo legítimo tiverem falhado (necessidade) e o uso da força seja justificado (proporcionalidade) ao nível da importância do objetivo legítimo (legalidade) a ser alcançado.

O Manual de Tallinn surgiu da necessidade de ultrapassar a desadequada aplicação dos normativos existentes, tais como a CNU, a um ciberataque ou a qualquer conflito cibernético, a fim de um qualquer Estado, por exemplo, recorrer ao uso da força para repelir uma ameaça ou um ataque, na perspetiva de legítima defesa.

Como tal, constatamos a indispensabilidade da interpretação dos tratados, bem como das suas deficiências, no contexto cibernético. O primeiro caso tem a ver com o significado da expressão "uso da força" no art.º 2.º n.º 4 da CNU, no qual se prevê a proibição desse facto, sendo neste contexto o objeto e a finalidade desta norma suficientes para limitar as circunstâncias em que os Estados poderão recorrer à força para resolverem as suas diferenças. Porém, as opiniões dos especialistas são divergentes em concordarem que uma ciber operação perpetrada por um Estado contra outro possa causar a lesão ou a morte a pessoas, danos ou destruição de propriedade, e que se enquadre no contexto do uso da força.

Já o segundo caso está relacionado com o art.º 5.º da CNU, o qual prevê que os Estados possam usar a força em resposta a um "ataque armado", sendo o seu objeto e finalidade evitar que os Estados permaneçam normativamente indefesos, caso o regime de execução estabelecido na Carta não funcione como planeado. A questão neste artigo prende-se com a interpretação efetuada do direito de autodefesa, em relação a ataques realizados por atores não-estatais, ou se os Estados se limitam a medidas de aplicação da lei na resposta a tais atos hostis. Esta questão no ciberespaço é vital, uma vez que é muito mais provável no contexto cibernético do que numa operação cinética, um grupo não-estatal ou um indivíduo terem a capacidade para lançar uma operação cibernética hostil contra um Estado, ao nível de um ataque armado, devido à relativa facilidade de adquirir os conhecimentos e equipamentos para um ataque armado cibernético em comparação com um cinético.

Noutro ponto de vista, afirma-se que o direito internacional é independente da tecnologia, motivo pelo qual não há razão para excluir as atividades cibernéticas do seu âmbito, pelo que, a UE na sua Estratégia de Segurança Cibernética de 2013 se comprometeu a aplicar o direito internacional existente no ciberespaço. Da mesma forma, a Declaração da Cúpula de Gales da OTAN de 2014 reconheceu que o direito internacional se aplica a atividades cibernéticas. Esta continua a ser a posição dominante, quer nestas organizações, quer em muitos países individuais semelhantes.

A globalização acarretou novos desafios tecnológicos, o que implica a utilização de diversos meios e a fixação de diversos objetivos, tais como a criação de uma estratégia de ciberdefesa, após o reconhecimento do ciberespaço como um domínio da guerra.

Face ao exposto, verifica-se uma proibição de ameaça ou uso da força, pelo que só poderá ser realizada uma operação cibernética quando estivermos perante uma ameaça ilegal ou o uso da força contra a integridade territorial ou independência política de qualquer Estado, bem como de qualquer outra maneira incoerente com os propósitos das NU, considerando que o direito internacional se aplica totalmente às atividades no ciberespaço.

Por outro lado, o mais recente Manual de Tallinn 2.0 assinalou a necessidade de dar cobertura às situações da ciberguerra em períodos de paz, através da lei internacional, pelo que atualmente se aceitou o âmbito mais vasto das ciberoperações, em detrimento do restrito âmbito dos ciberataques. Assim, esta versão do Manual contempla os aspetos chave do DIP, ao mesmo tempo que regula as ciberoperações durante o período de paz.

Em relação aos princípios da guerra clássicos, no âmbito de uma ação de ciberguerra no ciberespaço, destacamos o princípio do objectivo, princípio da ofensiva, princípio da massa, princípio da manobra, princípio da segurança, princípio da surpresa e o princípio da simplicidade, assumindo menor importância o princípio da economia de forças e o princípio da unidade de comando (por enquanto).

Por outro lado, a obtenção de uma capacidade tecnológica no domínio da segurança é essencial para a ciberdefesa, pelo que são exigidas estruturas próprias de ciberdefesa e cibersegurança, a fim de antecipar ataques desta natureza, ou mesmo e perpetrar ataques cibernéticos num conflito armado em coordenação ou não com outros teatros de operações.

Com efeito, reconhecemos que as operações de ciberguerra se assumem como um método para desenvolver e potenciar as operações militares, possibilitando realizar guerras no ciberespaço.

Conclusões

Ao longo do trabalho foi feita uma análise sumária à problemática do uso da força na Guerra mais convencional, analisou-se a segurança no ciberespaço e os respetivos ilícitos criminais, ao nível europeu (em particular na Estónia) e nacional, bem como as questões relativas ao terrorismo e ciberterrorismo. Em suma, procurou-se abordar e analisar o enquadramento legal do uso da força no ciberespaço, os princípios da guerra convencional, bem como a aplicação destes últimos no ciberespaço.

A problemática do uso da força no Direito Internacional Público não é algo recente, muito pelo contrário. Assim, já antes do século XX, a aceitação do uso da força no plano das relações internacionais era orientado pelo *jus ad bellum* (termos e condições da decretação do estado de guerra) e pelo *jus in bello* (normas reguladoras).

Mais recentemente, o uso da força no plano internacional assume-se como um poder exclusivo interno e externo do CS das NU, o qual detém igualmente o monopólio da aplicação de sanções segundo o princípio da proporcionalidade.

Como foi possível verificar está vedado o uso da força por parte de qualquer Estado, a não ser no caso de este ser em legítima defesa, apesar de carecer de uma "legitimação" do seu uso por parte da ONU, e de acordo com a CNU.

Todavia, antes da criação da ONU em 1945 não existia um regime eficaz o uso da força no Direito Internacional, pelo que com a CNU foi estabelecido um princípio da proibição do uso da força consagrado no seu art.º 2.º, n.º 4, o qual foi concretizado na sequência da II Grande Guerra pelas consequências nefastas para a sociedade.

Tal, assenta na premissa do art.º 1.º da CNU que preconiza a necessidade de manter a paz e a segurança internacionais, e para esse fim tomar as medidas coletivas internacionais para manter a paz, para prevenir e afastar ameaças à paz, atos de agressão ou qualquer rutura da paz e chegar por meios pacíficos a um ajustamento ou solução das controvérsias que possam levar a uma perturbação da paz.

O referido art.º 2.º, n.º 4, da CNU veio então definir a proibição do uso da força, sendo que não se refere apenas ao uso, mas também à ameaça contra a integridade territorial ou a independência política de um Estado. O mesmo deverá ser conjugado com o n.º 3 que versa a resolução pacífica de controvérsias. Esta norma é considerada uma norma *ius cogens* que significa ter natureza imperativa, inderrogável, aceite e reconhecida pela comunidade internacional de acordo com a Convenção de Viena sobre os Direitos dos Tra-

tados de 1969, a qual é válida para todos os Estados incluindo para os não membros da ONU.

Neste contexto, um órgão central é o CS das NU. Assim, nos termos do art.º 7.º, n.º 1, entre os principais órgãos da ONU encontra-se o CS como guardião da paz e segurança internacionais (art.º 24.º). De igual modo, refira-se que a CNU detém um valor substantivo inalienável pelo facto de ter permitido a *cristalização* do Direito Internacional, apesar de ter algumas insuficiências normativas, uma vez que o sistema onusiano não tem conseguido impedir o uso da força para além dos parâmetros jurídico-normativos estabelecidos.

Deste modo, constatamos a existência de uma proibição internacional do uso da força, de acordo com o art.º 2º, n.º 4, da CNU. Porém, esta proibição levanta alguns problemas: a interpretação do artigo de proibição do uso da força é controversa; existe uma divergência na prática estadual e na doutrina; há uma dificuldade em distinguir entre o uso da força lícita e ilícita nas relações internacionais; e a violação deste princípio é recorrente.

A proibição geral do uso da força apresenta como exceções, formalmente previstas, as seguintes: a legítima defesa; as medidas adotadas ou autorizadas pelos órgãos competentes da ONU para manter ou restabelecer a paz e a segurança internacionais; as medidas adotadas contra anteriores Estados inimigos; e as medidas adotadas por organizações regionais.

A situação do uso da força em legítima defesa assume-se como uma exceção à proibição do uso da força legítima, a qual terá de ser sempre exercida de acordo com o princípio da proporcionalidade, uma vez que se considera tratar-se de um *mecanismo de justiça privada* ao nível dos conflitos internacionais, até que o CS tome as medidas necessárias.

Na prática, o instituto da legítima defesa assume um caráter provisório, pelo que, quando exercido, este deve ser de imediato comunicado ao CS e terá como efeito o uso da força para repelir o ataque armado.

Todavia, para o exercício da legítima defesa terão de se verificar alguns pressupostos, tais como, a existência de um ataque armado ilícito contra o regime político e a integridade territorial de um Estado, atual ou iminente, ou seja, tal como nos casos de invasão, ataque armado, ocupação ou anexação, bombardeamento, ou bloqueio marítimo.

O direito de legítima defesa pode assumir uma vertente individual ou coletiva (exercido pelo próprio ou por terceiros) no caso de ocorrer um ataque armado, condição essencial para se recorrer a este direito. O mesmo tem lugar até que o CS tenha tomado as medidas necessárias para a manutenção da paz e segurança internacionais, não obstante este direito não depender de autorização do CS, mas extinguir-se logo que este intervenha.

Deste modo, o Direito Internacional estabelece a base normativa orientadora do recurso ao uso da força de modo legítimo por parte dos Estados, considerando que o uso da mesma nas relações internacionais não pode ser efetuado de forma arbitrária.

O uso da força tem de ser proporcional e necessário, uma vez que terá de se verificar uma correlação legítima entre a agressão e os meios adequados e necessários, caso não haja uma alternativa mais pacífica para a resolução do conflito.

Em Portugal, o Estado detém o monopólio do uso da força, pelo que o seu papel na Segurança Interna se revela fundamental, uma vez que este se constitui como um instrumento indispensável ao Estado, no sentido do *monopólio da violência física legítima*. Contudo, o seu uso terá de ser sempre proporcional nos meios a utilizar, não sendo admissíveis excessos, sob o risco de não respeitar os pressupostos da legítima defesa.

Por outro lado, o DIH estabelece o regime de tratamento de feridos e doentes militares, prisioneiros de guerra e populações civis em tempo de conflito armado, bem como distingue a situação de guerra do estatuto de neutralidade, pelo que este Ramo do Direito assume como objetivos: limitação do uso da força; proibição de armas bacteriológicas, químicas, gases asfixiantes ou tóxicos; proteção de bens culturais; e humanização dos prejuízos da guerra.

No que respeita às sanções coativas militares, previstas no art.º 42.º da CNU, se o Conselho concluir que as medidas do art.º 41.º não foram adequadas, poderá utilizar forças aéreas, navais ou terrestres para manter ou restabelecer a paz.

O recurso a estas sanções militares tem por base um sistema de segurança coletiva (art.º 33.º ao 38.º da CNU), o qual numa primeira fase pode apenas tomar decisões, a partir do art.º 39.º, após a constatação de uma ameaça à paz, rutura à paz ou ato de agressão.

O uso da força em legítima defesa (art.º 51.º da CNU) constitui-se como uma exceção à proibição do uso da força. Todavia, a legítima defesa encerra alguns constrangimentos, a saber: os problemas jurídicos que dificultam a licitude perante entidades não estatais; o pressuposto necessário de estar a ocorrer ou ter ocorrido; considerar-se um ataque armado contra a integridade territorial dos Estados; e a dificuldade em determinar a sua escala.

A título de exemplo, refira-se que os ataques terroristas não se enquadram no conceito de legítima defesa, embora as consequências possam ser igualmente devastadoras. Deste modo, verificamos que os ataques executados por entidades não estatais não se encontram previstas na CNU, porém, após os ataques do 11 de setembro, os EUA consideraram os ataques como um ataque armado e exerceram legítima defesa. Neste contexto, o CS acabou por reconhecer que se tratou de um ataque armado e que os EUA tinham legitimidade para

recorrer ao uso da força em legítima defesa, de acordo com o estatuído na resolução 1368 (2001), de 12 de setembro de 2001, do CS das NU, que condenou categoricamente estes atos e definiu a indispensabilidade de combater todas as formas de terrorismo, em conformidade com as responsabilidades consagradas na CNU.

Por outro lado, verificamos a ausência de uma definição clara de ataque armado, ao qual acrescentamos que atualmente os ataques não estão normalmente associados a Estados, situação que dificulta a atribuição da responsabilidade nos casos de terrorismo.

Em complemento, registemos que também não existe uma definição dos conceitos de ameaças à paz, rutura da paz e agressão, pelo que a interpretação e a prática não têm sido uniformes. Porém, o conceito de agressão pode ser entendido como o uso da força armada por um Estado contra a soberania, a integridade territorial ou a independência política de outro Estado, ou de qualquer outra forma incompatível com os princípios da Carta. O crime de agressão foi definido na Conferência de Kampala, onde a responsabilidade criminal é somente atribuída a indivíduos que se encontrem numa posição de efetivamente exercer controlo e dirigir uma ação política ou militar de um Estado.

Todavia, este uso da força obedece a requisitos diferentes, caso estejamos a falar do seu uso no ciberespaço, considerando a sua volatilidade e a dificuldade em se assacarem responsabilidades seja a um Estado ou a qualquer outro ator de relações internacionais. Nesta perspetiva, assume particular importância a problemática da prova digital, bem como a dificuldade na obtenção da mesma. Logo, se relacionarmos esta dificuldade com a necessidade de termos a certeza de quem cometeu uma qualquer ameaça ou ilícito criminais, dificulta ainda mais a legitimação do uso da força, porquanto cada dia mais se verifica uma maior probabilidade de ocorrer um ciberataque, seja ele contra pessoas, contra organizações ou mesmo contra Estados, tal como vimos com o exemplo da Estónia. Assim, é fulcral a adoção de estratégias de prevenção, de forma a minorar os respetivos danos, e caso não seja suficiente a prevenção, estarmos preparados para pudermos minorar os efeitos, que poderão ser verdadeiramente catastróficos.

As ameaças dissimuladas que circulam diariamente na internet, decorrentes da interdependência das suas redes e das infraestruturas informáticas, levam a que todos tenhamos de ter comportamentos preventivos, individuais, corporativos ou institucionais, no sentido de manter a disponibilidade e a integridade das redes e infraestruturas (sobretudo as críticas), bem como a confidencialidade das informações nelas contidas.

Contudo, a prevenção para ser eficaz requer uma boa *Intelligence*, seja ela HUMINT, OSINT ou outra qualquer, e uma consistente análise e gestão de risco, através dos referenciais normativos existentes já hoje.

No que concerne à cibersegurança, de uma forma simples, podemos assumir que a segurança interna fica encarregue do combate ao cibercrime e da proteção de IC, ao passo que à DN caberá a militarização do ciberespaço e o garante da soberania nacional.

De igual modo, diga-se que o ciberespaço não apresenta uma fronteira claramente definida do mundo real, porquanto, apesar de existir em diferentes domínios e com diferentes responsabilidades, um qualquer caso pode evoluir e requerer a atuação dos vários domínios, considerando que pode iniciar-se como um simples incidente de segurança e escalar para uma situação de crise, como por exemplo, se estiver a ocorrer um incidente numa infraestrutura crítica.

Assim, a LC é o *farol* que nos conduz na área da cibercriminalidade em Portugal. Porém, aliada à real dificuldade de investigação neste domínio, teremos sempre um tipo de criminalidade que tem as suas armas no anonimato e na alta tecnicidade dos meios empregues, entre outros. Esperemos, pois, que no futuro essa opacidade na qual os ciber agentes atuam dê progressivamente lugar à transparência, neste caso entendida como possibilidade de rastrear como mais facilidade o tráfego, pois a tecnologia é capaz de quase tudo.

Em relação ao combate ao cibercrime, algumas das questões importantes passam pela proteção do património e das pessoas, pelo que deverá ocorrer a criminalização dos ataques contra os sistemas informáticos e a informação neles contida. De igual modo, importa assegurar um nível adequado de segurança para os utilizadores das TIC, ao mesmo tempo que a atualização legislativa das matérias do ciberespaço tem de acompanhar o ritmo vertiginoso com que os ciberataques e as respetivos métodos de ataque se vão transformando.

Noutro patamar, os ciberataques poderão ser encarados como um ato de Guerra, pondo em risco a existência do Estado, em particular a sua soberania, uma vez que estes têm como objetivo eliminar uma ameaça que coloque em causa a soberania nacional ou ganhar uma vantagem competitiva sobre outro Estado.

Neste contexto, e após os ciberataques da Estónia, surgiu o Manual de Tallinn em 2008, fruto da necessidade de serem estabelecidas regras internacionais básicas para a ciberguerra, tendo sido publicado sob a direção da OTAN, numa primeira tentativa de transpor as leis internacionais para a ciberguerra.

Este Manual foi criado após os ciberataques de que este país tinha sido vítima no ano anterior, os quais tinham tido como alvos o Governo, instituições financeiras e os *media* do

país. Trata-se de um extenso Manual que define as condições em que um país pode responder a um ciberataque com forças militares, tendo sido o primeiro a pretender orientar a definição da legitimidade para a ciberguerra, tendo por base os princípios das Leis internacionais, do respeito pela soberania dos Estados e da defesa dos Direitos Humanos, ressalvando-se a proibição de ameaça ou uso da força. Assim, só poderá ser realizada uma operação cibernética quando estivermos perante uma ameaça ilegal ou o uso da força contra a integridade territorial ou independência política de qualquer Estado, bem como de qualquer outra maneira inconsistente com os propósitos das NU, pelo que se pode afirmar que o direito internacional se aplica totalmente às atividades no ciberespaço.

O recurso ao uso da força apenas se pode verificar quando todos os outros meios de alcançar um objetivo legítimo tiverem falhado (necessidade) e o uso da força seja justificado (proporcionalidade) pela importância do objetivo legítimo (legalidade) a ser alcançado.

A atual estruturação das sociedades em rede é uma evidência do seu grau de desenvolvimento, apesar desta dependência do ciberespaço acarretar o aparecimento de vulnerabilidades que devem ser mitigadas, devido às mesmas conduzirem ao Cibercrime.

Em relação às ameaças ao ciberespaço, ou à realidade que o mesmo engloba, podem ser várias e estão divididas na literatura essencialmente em cinco dimensões: o cibercrime, o hacktivismo, o ciberterrorismo, a ciberespionagem e a ciberguerra.

Neste contexto, teremos de ter uma ciberdefesa capaz de assegurar a segurança dos meios intrínsecos de cada Estado, devendo, para tal, usar todos os meios disponíveis para garantir a soberania do Estado, nomeadamente em situações de crise ou de guerra.

Tal, decorre do facto de o ciberespaço se assumir como uma extensão virtual do mundo físico em que vivemos. Neste ambiente virtual, o ciberespaço é suportado através de uma rede mundial de computadores interligados pela infraestrutura de comunicações, no qual se realizam diversas interações entre pessoas ou agentes de *software*, permitindo uma comunicação global e com o objetivo principal de partilhar informação.

Noutra vertente, a ciberguerra pode ser definida como um ato de guerra entre grupos políticos, no ciberespaço, o qual se destina a submeter o adversário à sua vontade, bem como visa determinado fim político.

Esta reconhecida componente de ciberguerra conduziu a uma alteração do paradigma tradicional dos cenários de conflito e domínios operacionais (terra, mar, ar e espaço), os quais estão diretamente relacionados com os riscos e as ameaças à Segurança e Defesa Nacional. Neste contexto, o ciberespaço surge como quinto domínio operacional.

Esta importância operacional atribuída ao ciberespaço acarreta uma responsabilidade acrescida dos diversos atores em desenvolver novas estratégias, doutrinas e capacidades, o que implica a necessidade de uma melhor edificação das capacidades de cibersegurança e ciberdefesa. Para tal, afigura-se pertinente a promoção de estratégias de cooperação dos diversos atores, seja no plano nacional ou internacional, e contribuir para uma visão integradora e sinérgica dos esforços a desenvolver. De igual modo, terá de ser desenvolvida uma cultura estratégica de cibersegurança e ciberdefesa, na qual se inclui a gestão de crises no ciberespaço de forma eficaz e eficiente, bem como se garanta a utilização segura do ciberespaço, em particular no que respeita à proteção das suas infraestruturas críticas e das informações dos cidadãos, através da adoção de mecanismos e ferramentas adequadas.

O ciberespaço assume uma constante mutação do seu mundo virtual, situação que leva ao aumento da dificuldade da sua proteção e da inerente evolução legislativa.

Por outro lado, temos assistido ao surgimento de "novas ameaças" de cariz assimétrico e a uma desterritorialização do conceito de Defesa, motivos que têm revelado uma obrigação dos Estados em estabelecerem uma Estratégia da Informação.

Nesta perspetiva, as previsões de guerra num futuro próximo apontam para a mesma seja iniciada num ataque cibernético maciço, para desorganizar as capacidades do inimigo.

Como tal, temos assistido ao desenvolvimento de mecanismos de proteção e defesa com o objetivo de garantir a segurança no ciberespaço, com os Estados a reconhecer a importância do desenvolvimento de políticas e estratégias cooperativas de combate a ataques cibernéticos, materializadas em iniciativas de caráter nacional e internacional. Neste sentido, a UE tem desenvolvido esforços nas áreas da cibersegurança e da ciberdefesa.

Tal, assenta nas ameaças e principais riscos ligados à criminalidade na Europa, tais como o terrorismo, as graves formas de criminalidade organizada, a cibercriminalidade, o tráfico de armas e a criminalidade transfronteiriça, os quais se adaptam a uma velocidade extraordinariamente rápida à evolução da ciência e da tecnologia. Neste particular, a cibercriminalidade é uma realidade em permanente mutação e em evolução constante, sendo potenciada pelo ambiente do ciberespaço através do anonimato, da dificuldade de definição da jurisdição e da extraterritorialidade.

No que concerne às principais dificuldades da investigação da cibercriminalidade, estas assentam no seguinte: interpretação dos diplomas *à la carte*; transnacionalidade; cooperação internacional morosa ou não existente; evolução técnica versus adaptação jurídica.

Com efeito, verifica-se uma necessidade de uniformização internacional das leis do ciberespaço, em particular da sua moldura penal, bem como de identificação das técnicas

mais eficazes de combate à cibercriminalidade, a fim de serem prevenidos e mitigados os riscos e perigos da utilização do ciberespaço, em particular, no que se refere ao funcionamento da rede e das infraestruturas críticas e da segurança dos seus utilizadores.

Neste contexto de incerteza, vai-se gerando um sentimento de insegurança ao nível mundial, particularmente como consequência da facilidade com que se consegue explorar as vulnerabilidades das sociedades modernas, organizadas em rede e com as estruturas críticas apoiadas no ciberespaço. Para a sua mitigação é necessário ser capaz de coordenar a resposta operacional a ciberataques, desenvolver sinergias nacionais e potenciar a cooperação internacional neste domínio, bem como desenvolver as capacidades de ciberdefesa.

No que concerne ao ciberterrorismo, algumas das preocupações alicerçam-se nas questões da admissibilidade e autenticidade da prova, porquanto a aplicabilidade do direito aos atos eletrónicos apresenta limitações como a competência territorial e a dificuldade em estabelecer uma previsão legal dos seus mecanismos. Tal, assenta na falta de adequação das atuais normas penais aos critérios da territorialidade e materialidade da prática dos crimes, em contraponto com o caráter transfronteiriço e virtual dos atos praticados.

Neste sentido, deixamos aqui algumas preocupações que deveriam merecer uma reflexão, no sentido da necessária revisão legislativa e procedimental das problemáticas da cibersegurança, do cibercrime, da ciberdefesa e do ciberterrorismo, a saber: implementação de uma estratégia nacional de cibersegurança que junte as competências dos diversos atores políticos e operacionais, incluindo as FA e as FSS; alargamento do âmbito da Lei Criminal ao espetro dos crimes cometidos no ciberespaço, adequando igualmente a Lei de Organização da Investigação Criminal à necessária investigação dos crimes que ocorrem no ciberespaço, incluindo as diligências necessárias à preservação da cadeia de custódia da prova; o estabelecimento contínuo e dinâmico de sinergias entre os diversos atores nacionais e internacionais; a manutenção e desenvolvimento da cooperação internacional; implementação de instrumentos de política cibernética; a definição de uma agenda única do Cyber pelos vários instrumentos políticos atuais (a Estratégia de Segurança Interna, a Estratégia para o Mercado Único Digital, o Quadro de Política de Ciberdefesa, além da Estratégia de Segurança Cibernética da UE); assegurar uma nova abordagem que deverá ter como objetivo ter ações mais bem definidas e mais direcionadas que cubram todos estes novos instrumentos legislativos; atualização sobre o progresso de desenvolvimento de tecnologias e ferramentas forenses digitais adequadas, tendo em vista a evolução do combate ao cibercrime; criação de um modelo para a legislação relativa ao crime cibernético nacional em todas as instâncias competentes; e criação de procedimento doutrinários que regu-

lem e implementem o uso da força no ciberespaço, mas de uma forma integrada, através da cooperação internacional e da aceitação destas normas pela maioria dos países do mundo.

Nesta perspetiva, os desafios de *governance* ou de natureza legal passarão pelo desenvolvimento de capacidades e enquadramento legal que nos permita conseguir dar uma melhor resposta a estes fenómenos, que se assumem como mutáveis e de difícil previsão. Só a implementação de uma estratégia preventiva e com capacidade de resposta operacional a ciberataques poderá evitar ou minimizar o uso da força, sendo fulcral para tal desenvolver sinergias nacionais e potenciar a cooperação internacional neste domínio.

Noutro sentido, e de acordo com o nosso caso de estudo, verificámos que no caso dos ciberataques na Estónia a maioria dos Princípios da Guerra clássicos se revelaram importantes para uma ação de ciberguerra, à exceção do princípio da economia de forças e do princípio da unidade de comando. Deste modo, constata-se que o princípio do objectivo, princípio da ofensiva, princípio da massa, princípio da manobra, princípio da segurança, princípio da surpresa e o princípio da simplicidade são todos importantes para uma ação de ciberguerra no ciberespaço. Porém, o princípio da unidade de comando será certamente um princípio a ter em conta quando se verificar a criação dos centros de ciberdefesa.

Com efeito, a ciberguerra implica a obtenção de uma capacidade tecnológica no domínio da segurança, exigindo estruturas próprias de ciberdefesa e cibersegurança, com vista a antecipar ataques desta natureza, ou mesmo e perpetrar ataques cibernéticos num conflito armado em coordenação ou não com outros teatros de operações. Como tal, concluímos que os Princípios da Guerra continuam atuais e relevantes para ações de ciberguerra e podem ser aplicáveis e usados na ação de comando e controlo dos chefes militares, pelo que as ações de ciberguerra no ciberespaço podem ser planeadas tendo em consideração o princípio do objectivo, princípio da ofensiva, princípio da massa, princípio da manobra, princípio da segurança, princípio da surpresa e o princípio da simplicidade, de modo a orientar a ação de comando dos chefes militares nas respetivas operações de ciberguerra.

De igual modo, a ciberguerra assume-se como um novo método para desenvolver Operações Militares no ciberespaço, o qual engloba um conjunto de ações (CNA, CND e CNA) que são desenvolvidas com o intuito de atingir determinado fim político.

Face ao exposto, deixamos as nossas respostas às hipóteses formuladas:

H1: As ciberameaças não condicionam diretamente o recurso ao uso da força à luz do Direito Internacional, não obstante dificultarem a sua tipificação e aplicação.

H2: O uso da força no ciberespaço é feito com base na CNU, mas também noutro tipo de diplomas legais e à luz de boas práticas, tal como é o caso do Manual de Tallinn.

H3: A legítima defesa pode ser feita por qualquer Estado que sofra um ataque armado no âmbito da Guerra Cibernética, apesar de posteriormente o CS das NU ter de legitimar o uso da força para se efetivar legalmente o conceito de legítima defesa, sendo vital para tal que a ameaça ainda se mantenha atual e iminente.

H4: O Manual de Tallinn vai ajudar à criação de uma Estratégia de implementação de um plano de ação para o combate ao cibercrime, considerando que é elaborado por um grupo multidisciplinar de individualidades independentes convidadas para o efeito, e abarca vários setores de atividade.

Para concluir, deixamos aqui algumas propostas futuras que deverão ser tidas em consideração, uma vez que é do conhecimento geral que urge a necessidade de revisão legislativa desta problemática da cibersegurança e, consequentemente, do cibercrime, bem como adequar os considerandos clássicos do uso da força à realidade atual do ciberespaço, nos termos de uma Convenção ou Tratado Internacional específica para as questões do ciberespaço.

Bibliografia

Livros:

- ALMEIDA, Cláudia – A Problemática da Cibersegurança: o Caso da Estratégia Nacional de Segurança no Ciberespaço. In **III Seminário IDN Jovem.** N.º 30. Lisboa: IDN, [s.d.]. p. 271-288.
- ALMEIDA, Ivo – **A Prova Digital.** Lisboa: Universidade Autónoma de Lisboa, 2014. Dissertação de Mestrado.
- ALVES, David – **Uso excessivo da força. Questões jurídicas, técnico-policiais e sociais.** Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna, 2016. Dissertação de Mestrado.
- AMARAL, Sandra – **O Papel dos Serviços de Informações no Combate ao Ciberterrorismo: o Caso Português.** Lisboa: Academia Militar, 2014. Dissertação de Mestrado.
- ANTUNES, David – **O Hacktivismo e as Forças Armadas.** Lisboa: Instituto de Estudos Superiores Militares, 2013. Trabalho de Investigação Individual do CEMC – 2012/13.
- ARON, Raymond – **Paz e Guerra entre as Nações.** 2ª Ed. Brasília: Editora Universidade de Brasília, 1986.
- ARCHICK, K. – **Cybercrime: The Council of Europe Convention.** Budapeste: Conselho da Europa, 2005.
- ARQUILLA, John; RONFELDT, David – **A New Epoch – and Spectrum – of Conflict**. 2000.
- ASSANGE, Julian – **Cypherpunks. Liberdade e o futuro da internet.** Lisboa: Editempo Editorial, 2013.
- AZIZ, Ashar – **The Evolution of Cyber Attacks and Next Generation Threat Protection.** RSA Conference 2013, FireEye, Inc.
- BARBOSA, Maria – **As ameaças ao ciberespaço e a estratégia de segurança da UE e Portugal.** Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2016. Trabalho Individual.
- BAYLIS, John et al. – **Strategy in the Contemporary World.** 2nd Ed. Oxford: Oxford University Press, 2007. ISBN 978-0-19-928978-3.
- BETZ, David; STEVENS, Timothy – **Cyberspace and the State: Towards a Strategy for Cyberpower.** Routledge: The International Institute for Strategic Studies, 2011.

- BRANDÃO, Ana – As tendências Internacionais e a posição de Portugal. In **Actas.** I Congresso Internacional do OBSERVARE. Lisboa: Universidade Autónoma de Lisboa, 2011.
- BRAVO, Rogério – **As Tecnologias de Informação e a Compressão dos Direitos, Liberdades e Garantias: os efeitos das regras "10/10" e "1/1"**. 2012.
- BRAVO, Rogério – Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta. In **Revista Polícia e Justiça.** III Série. N.º 7. Janeiro-Junho 2008. Coimbra: Coimbra Editora, 2008.
- BURRUSS, George W.; HOLT, Thomas J.; BOSSLER, Adam M. – Exploring the Utility of Open Source Data to Predict Malicious Software Creation. **Cyber Infrastruture Protection.** Vol. II. U.S. Army War College Press. 2013. ISBN 1-58487-571-2. p. 183-218.
- CALDAS, Alexandre; FREIRE, Vicente – **Segurança Internacional: Perspetivas Analíticas.** Lisboa: Imprensa Nacional – Casa da Moeda/Instituto da Defesa Nacional, 2013.
- CASA BRANCA – **Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.** Washington: s.n., 2009.
- CASTELLS, Manuel – **A Sociedade em rede.** 2ª Ed. São Paulo: UNESP, 1999.
- CLARK, David; BERSON, Thomas; LIN, Herbert – **At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues.** Washington D.C. The National Academies Press, 2014.
- CAMPOS, Eduardo – **Acesso a dados pessoais de saúde contidos em ficheiros dos hospitais públicos: ponderação entre o direito de acesso à informação e aos documentos administrativos e o direito à protecção de dados pessoais: quem e como decide?** Lisboa: ISCTE – Instituto Universitário de Lisboa, 2009. Dissertação de Mestrado.
- CASA BRANCA – **Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.** Washington: s.n., 2009.
- CASIMIRO, Sofia – **A Responsabilidade Civil pelo Conteúdo da Informação Transmitida pela Internet.** Coimbra: Almedina. 2000.
- CHOPE, M. Christopher; KÕUTS, M. Tarmo – **CINQUANTE-CINQUIÈME SESSION - La guerre informatique.** 2008.
- CLAY, Wilson – **Cyberwarfare.** Washington DC: CRS Report for Congress, 2001.
- CLAY, Wilson – **Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues.** Washington DC: CRS Report for Congress, 2007.

- CLAY, Wilson – **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.** Washington DC: CRS Report for Congress, 2008.
- CLEMENTE, Pedro – **Da Polícia de Ordem Pública.** Lisboa: Governo Civil, 1998. Dissertação de Mestrado.
- CLEMENTE, Pedro – Polícia e Segurança – breves notas. In **Lusíada. Política Internacional e Segurança.** N.º 4, 2010. p. 139-169.
- COMISSÃO EUROPEIA - **Livro Verde: Relativo a um programa Europeu de protecção das infraestruturas críticas.** Bruxelas: s.n., 2005. COM(2005) 576 final.
- COMISSÃO EUROPEIA – **Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido.** Bruxelas: JOIN, 2013.
- CONSELHO EUROPEU **– Declaração sobre a luta contra o Terrorismo.** Bruxelas, 2004.
- CORNISH, Paul – **Cyber-Security and Politically, Socially and Religiously.** Brussels: European Parliament, 2009. PE 406.997.
- CORREIA, João – Prova Digital: as leis que temos e as que devíamos ter. In: **Revista do Ministério Público.** N.º 139 (Julho-Setembro), 2014. p. 29-59.
- COSTA, João – **A responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na Internet - Em especial da responsabilidade pelos conteúdos gerados por utilizadores** Porto: Faculdade de Direito da Universidade de Direito, 2011. Dissertação de Mestrado.
- COUTINHO, Francisco – A Proibição do Uso da Força no Século XXI. In CALDAS, Roberto et. al. – **Guerra e Paz no Século XXI: políticas e direito internacional.** Coimbra: Almedina, 2018. p. 83-100.
- CUSTÓDIO, Vitor – Uma viagem através do Ciberespaço. In: **Revista A Mensagem.** Lisboa: Regimento de Transmissões, 2016. p. 42-45.
- Decreto-Lei n.º 69/2014. **Diário da República I Série.** N.º 89 (09-05-2014). p. 2712-2719.
- DEFENCE, Federal Ministry Republic of Austria – **Handbook on Cybersecurity. The Common Security and Defence Policy of the European Union.** Vol. V. 1ª Ed. Luxembourg: Publications Office of the European Union, 2018. ISBN 978-92-95201-12-5.
- DÉFENSE ET SÉCURITÉ NATIONALE – **Le Livre Blanc.** Paris: Odile Jacob, 2008.
- Despacho n.º 13692/2013. **Diário da República II Série.** N.º 208 (28-10-2013). p. 31976-31979.

- DIAS, Vera – A Problemática da Investigação do Cibercrime. In: **Data Venia. Revista Jurídica Digital.** ISSN 2182-6242. N.º 1 (Julho-Dezembro), 2012. p. 63-88.
- DINSTEIN, Yoram – **Guerra, Agressão e Legítima Defesa.** São Paulo: Manole, 2004.
- DINSTEIN, Yoram – **The Conduct of Hostilities under the Law of Armed Conflict.** UK Ministry of Defence, The Manual of the Law of Armed Conflict. Oxford: Oxford University Press, 2004.
- DIULIANE, Ellen – **A proteção de dados pessoais e privacidade do utilizador no âmbito das comunicações eletrónicas**. Lisboa: Universidade Autónoma de Lisboa, 2015. Dissertação de Mestrado.
- DOMINGUES, Elisabete **– Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo.** Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna, 2015. Dissertação de Mestrado.
- DONEDA, Danilo – **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. ISSN 2179-7943.
- DRUCKER, Peter – **Management Challenges for the 21st Century.** Harper Business, 1999. ISBN: 13-978-0887309991.
- DUARTE, Vânia – **Protecção de dados pessoais na internet: o caso do "direito a ser esquecido".** Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2014. Dissertação de Mestrado.
- ELIAS, Luís; GUEDES, Armando – **Controlos Remotos: Dimensões Externas da Segurança Interna em Portugal.** Lisboa: Almedina, 2010. ISBN 9724043576.
- ENISA – **Report on Cyber Crisis Cooperation and Management.** European Union Agency for Network and Information Security, 2014. ISBN: 978-92-9204-100-7.
- ESCARAMEIA, Paula – **Guerra do Iraque – Fundamentos Jurídicos do Uso da Força.** Lisboa: Instituto Superior de Ciências Sociais e Políticas, Universidade Técnica de Lisboa, 2003.
- ESCARAMEIA, Paula **– O tribunal penal internacional e o crime de agressão.** Lisboa: Faculdade de Direito da Universidade Católica Portuguesa, 2006.
- FERNANDES, Filipe – **A Cibersegurança e as Estruturas Críticas: A GNR. Ciberguarda, o Futuro.** Lisboa: Academia Militar, 2013. Dissertação de Mestrado.
- FERNANDES, Jorge – **Gestão da segurança da informação e comunicações.** Vol. 1. Brasília: Universidade de Brasília, Faculdade de Ciência da Informação, 2010. Série Segurança da Informação. ISBN 978-9949-9211-2-6.

- FERNANDES, José – A ciberguerra como nova dimensão dos conflitos do século XXI. In **Relações Internacionais.** Nº 33. 2012. (março) ISSN 1645-9199.
- FERREIRA, Pedro – **A Proteção de Dados Pessoais na Sociedade de Comunicação - Dados de Tráfego, Dados de Localização e Testemunhos de Conexão.** Lisboa: O Espírito das Leis, 2006. p. 71.
- FERREIRA-PEREIRA, Laura – **A Política Europeia de Segurança e Defesa após o Tratado de Lisboa: estado da arte e perspectivas futuras.** KA Cadernos 2013.
- FERREIRA, Renato – Globalização e Segurança. Um mundo em mudança. In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 8 Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2015.
- FM 3-38 – **Cyber Electromagnetic Activities**, p. 1-8.
- FREIRE, Fernando; NUNES, Paulo – Estratégia da Informação e Segurança no Ciberespaço. In **Estratégia da Informação e Segurança no Ciberespaço**. 2013. Vol. 12. Lisboa: Instituto de Defesa Nacional, IDN Cadernos. ISBN: 978-972-27-2272-8. p. 9-94.
- FREITAS, Joana – "Novas Armas, Nova Lei?": Ensaio sobre a aplicação do Direito Internacional Humanitário à Guerra Cibernética. A Problemática do Princípio da Distinção num Mundo Interconectado. In **Revista de Ciências Militares** Vol. I. N.º 2. Novembro 2013. p 49-67.
- FRIAS, Óscar – **Cyber Intelligence. A obtenção de Informações a partir de fontes abertas no Ciberespaço.** Lisboa: Academia Militar, 2013. Dissertação de Mestrado.
- GIBSON, William – **Neuromancien.** Paris: La Découverte, 1985.
- GINKEL, B.– **Responding to Cyber Jihad: Towards an Effective Counter Narrative.** 2015.
- GONÇALVES, João – A prova digital em 2017 – Reflexões sobre algumas insuficiências processuais e dificuldades da investigação In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 57 Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2017.
- GOUVEIA, Jorge – **Direito Internacional Penal, Uma perspetiva dogmático crítica.** Coimbra: Almedina Editora,2008. ISBN 9789724035932.
- GOUVEIA, Jorge – O uso da força no Direito Internacional Público. In **Revista Brasileira de Estudos Políticos.** N.º 107. Belo Horizonte: 2013. (julho/dezembro). p. 149-200.
- GOUVEIA, Jorge – **Direito da Segurança. Cidadania, Soberania e Cosmopolitismo.** 1ª Ed. Coimbra: Almedina Editora, 2018. ISBN 978-972-40-7492-4;

- GOUTAM, R. – **Importance of Cyber Security.** International Journal of Computer Applications, 2015. 111(7). p. 14-17.
- GUEDES, Armando – **As "redes sociais" digitais, a participação "política" e a segurança.**
- GUEDES, Armando; SANTOS, Lino – Breves reflexões sobre Poder e Ciberespaço. In **Revista de Direito e Segurança**. N.° 6 (julho / dezembro de 2015). p. 189-209.
- GUERRA, Amadeu – Lei de Proteção de Dados Pessoais. In **Estratégia da Informação e Segurança no Ciberespaço**. 2013. Vol. 12. Lisboa: Instituto de Defesa Nacional, IDN Cadernos. ISBN: 978-972-27-2272-8.
- HAÏDAR, Tim – **Cyber 9/11: is the oil & gas industry sleepwalking into a nightmare?** Oil & Gas IQ, 2015.
- HARRIS, S. – **All in one CISSP exam guide.** 5th Ed. McGraw-Hill, 2010.
- HATHAWAY, Melissa; KLIMBURG, Alexander – The Five Mandates of National Cyber Security. In **National Cyber Security Framework Manual.** NATO CCD COE Publication, Tallinn 2012. ISBN 978-9949-9211-2-6.
- HERZOG, S. – **Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.** Journal of Strategic Security, 2011. 4(2), p. 49-60.
- INSTITUTO DA DEFESA NACIONAL – **Conceito Estratégico de Defesa Nacional – Contributos e Debate Público.** Lisboa: Imprensa Nacional – Casa da Moeda/Instituto da Defesa Nacional, 2013.
- INSTITUTO DA DEFESA NACIONAL – **Estratégia da Informação e Segurança no Ciberespaço.** N.º 12. Lisboa: Instituto da Defesa Nacional, 2013. ISBN: 978-972-27-2272-8.
- INTERNATIONAL AFFAIRS REVIEW. **Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security**. Washington: George Washington University, 2009.
- ITU – **Cybersecurity: The Role and Responsibilities of na Effective Regulator.** Beirut: ICT Applications and Cybersecurity Division, 2009.
- JORDAN, Tim; TAYLOR, Paul – **Hacktivism and Cyberwars: Rebels with a cause?** New York: Routledge, 2004.
- JP 2-01.3. – **Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace.** 2000.

- JP 1-02. – **Department of Defense Dictionary of Military and Associated Terms.** 2009.
- JUNIOR, Alberto – **O Direito de Assistência Humanitária.** Rio de Janeiro: Renovar, 2003.
- KLIMBURG, Alexander et al – **National Cyber Security: Framework Manual.** Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012.
- KREKEL, Bryan – **Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.** McLean: Northrop Grumman, 2009.
- LAGARES, Rodrigo – **O Processo de Transformação da Superioridade de Informação em Superioridade de Decisão**. Lisboa: Academia Militar, 2017. Dissertação de Mestrado.
- LARA, António – **O Terrorismo e a Ideologia do Ocidente**. Coimbra: Edições Almedina, 2007.
- LARA, António – **Ciência Política – Estudo da Ordem e da Subversão.** 6ª Ed. Lisboa: Instituto Superior de Ciências Sociais e Políticas, 2011.
- LE LIVRE BANC – **Défense et Sécurité nationale.** Paris: Odile Jacob, 2008.
- Lei N.º 46/2018. **Diário da República I Série.** N.º 155 (13-08-2018). p. 4031-4037.
- Lei N.º 53/2008. **Diário da República I Série.** N.º 167 (29-08-2008). p. 6135-6141.
- Lei n.º 72/2015. **Diário da República I Série.** N.º 139 (20-07-2015). p. 4909-4911.
- Lei N.º 96/2017. **Diário da República I Série.** N.º 162 (23-08-2017), p. 4924-4928.
- Lei N.º 109/2009. **Diário da República I Série.** N.º 179 (15-09-2009). p. 6319-6325.
- LEITE, Ana – A problemática da cibersegurança e os seus desafios. In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 49. Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2016.
- LEMOS, Elsa – ***Media*** **e a gestão da percepção nas novas conflitualidades.** Lisboa: Academia Militar, 2012. Dissertação de Mestrado.
- LIMA, Robson et al – **O Manual de Tallinn e a Regulação da Cibersegurança e Ciberguerra.** Lisboa: Instituto Universitário Militar, 2018. Trabalho de Aplicação de Grupo do CEMC 2017/2018.
- LIN, H. et al – **Toward a safer and more secure cyberspace.** 2007.
- LIVRO VERDE – **Livro Verde: Relativo a um programa Europeu de protecção das infraestruturas críticas.** Bruxelas: s.n., 2005. COM(2005) 576 final.

- LOPES, Francisco – **Gestão do Conhecimento – Modelação dos Incidentes e das Respostas.** Lisboa: Universidade Católica Portuguesa, Faculdade de Engenharia, 2010. Dissertação de Mestrado.
- LOPES, José – **Violência policial: o uso legítimo da força.** Lisboa: Academia Militar, 2006. Trabalho Final de Curso.
- LOSAVIO, Michael; SHUTT, J. Eagle; KEELING, Deborah – Changing the game: social and justice models for enhanced cyber security. In SAADAWI, Tarek; JORDAN JR., Louis; BOUDREAU, Vincent – **Cyber Infrastructure Protection.** Volume II. Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 2013. ISBN 1-58487-571-2.
- LOURENÇO, Ana – **Os perigos da utilização dos dados pessoais.** Lisboa: Universidade Autónoma de Lisboa, 2016. Pós-graduação em Protecção de Dados Pessoais e Direito à Privacidade.
- LOURENÇO, Nelson – As Novas Fronteiras da Segurança – Segurança Nacional, Globalização e Modernidade. In **Segurança e Defesa.** N.º 31. Lisboa: 2015 (fevereiro-junho).
- LOURENÇO et al. – **Segurança Horizonte 2025. Um Conceito Estratégico de Segurança Interna.** Lisboa: Edições Colibri, 2015.
- MACHADO, Paulo – **O Papel da GNR no Contexto da Cibersegurança Nacional.** Lisboa: Instituto de Estudos Superiores Militares, 2015. Trabalho de Investigação Individual do CEMC – 2014/15.
- MANUEL, A. – **A dimensão política da Segurança para o Ciberespaço na União Europeia**. Açores: Universidade dos Açores, 2014.
- MARQUES, Pedro – **Informática Forense. Recolha e preservação da prova digital** Lisboa: Universidade Católica Portuguesa. Faculdade de Engenharia, 2013. Dissertação de Mestrado.
- MARTINS, José – **Framework de Segurança de um Sistema de Informação.** Guimarães: Universidade do Minho, 2008. Dissertação de Mestrado.
- MARTINS, M. – Ciberespaço: uma Nova Realidade para a Segurança Internacional. In **Nação e Defesa** – Lisboa: Instituto Da Defesa Nacional, 2012.
- MASSENO, Manuel – Garantira Cibersegurança e a Ciberdefesa à custa dos Cidadãos? In **IX Simpósio sobre Segurança Informática e Cibercrime.** SimSIC: Beja, 2018.
- MASSENO, Manuel **– Segurança e Liberdade na Sociedade Global em Rede.** [s.d.].
- MATIAS, A. – **A Violência no Mundo Moderno**. Lisboa: Livraria Bertrand, 1978.

- MAXIMIANO, António – Qualidade de Acção policial. In **Seminário sobre parâmetros jurídicos da actuação Policial**. Lisboa: IGAI, 1996.
- MENEZES, Umbelina – **O Papel das Forças e Serviços de Segurança no Combate aos Crimes Cibernéticos em Angola.** Lisboa: Universidade de Lisboa, Faculdade de Direito, Instituto Superior Técnico, 2016. Dissertação de Mestrado.
- MILITÃO, M. – A violência na sociedade actual. In **Controlo externo da actividade policial e dos serviços tutelados pelo MAI.** Lisboa: Inspeção-Geral da Administração Interna, 2001. p. 295-302.
- MILITÃO, Octávio – **Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional.** Lisboa: Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa, 2014. Dissertação de Mestrado.
- MILLER, Arthur. **The assault on privacy.** Ann Arbor: University Of Michigan Press, 1971.
- MONIZ, Helena – **O Crime de Falsificação de documentos. Da falsificação intelectual e da falsificação em documento.** Coimbra: Coimbra Editora, 2004.
- MOREIRA, Adriano – **Ciência Política**. Coimbra: Almedina, 1997.
- MOREIRA, Adriano – **Teoria das Relações Internacionais.** 4ª Ed. Coimbra: Almedina, 2002.
- MOREIRA, Adriano – A estratégia global contra o terrorismo. In **Jornal Público.** Ed. 01 de julho de 2014. p. 46.
- MOREIRA, Adriano; RAMALHO, Pinto (coord.) – **Estratégia.** Vol. XIX. Lisboa: Instituto Português da Conjuntura Estratégica, 2010. ISSN 1645-9083.
- MOREIRA, João – **O Impacto Do Ciberespaço Como Nova Dimensão Nos Conflitos.** Boletim Ensino. Investigação n.º 13. Lisboa: Instituto Universitário Militar, 2012. p. 27-50.
- MURAWIEC, Laurent – La cyberguerre. In **AGIR - Revue Génerale de Stretégie. Révolution de l'information, crise de Communication.** N.º 2. 1999.
- NATÁRIO, Rui – **O Ciberespaço e a Vulnerabilidade das Infraestruturas Críticas: Contributos para um Modelo Nacional de Análise e Gestão do Risco Social.** Lisboa: Academia Militar, 2014. Dissertação de Mestrado.
- NATÁRIO, Rui; NUNES, Paulo – Risco Social no Ciberespaço. A Vulnerabilidade das Infraestruturas Críticas. In **Revista Militar.** N.º 2547 (Abril), 2014. p. 249-286.
- NISSENBAUM, H. – **Where computer security meets national security. Ethics and Information Technology.** 7(2). 2005.

- NYE, Joseph – **Cyber Power. Technical Report.** Belfer Center for Science and International Affairs, Harvard Kennedy School, 2010.
- NYE, Joseph – **O Futuro do Poder.** Lisboa: Círculo de Leitores, 2012.
- NOGUEIRA, Pedro – **Modelos híbridos de Segurança, o desafio da dimensão Público-Privada.** Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2016.
- NOVAIS, Rui – Media e (Ciber)Terrorismo. In **Cibersegurança**. N.º133. Lisboa: Nação e Defesa – Instituto de Defesa Nacional, 2012.
- NUNES, Paulo – **Novos Desafios da Segurança e Defesa no Ciberespaço.** Conferência PGEES, 2012.
- NUNES, Paulo – Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço. In **IV Simpósio sobre Segurança Informática e Cibercrime.** SimSIC: Beja, 2013.
- NUNES, Paulo – **Sociedade em rede, ciberespaço e guerra de informação.** Lisboa: Instituto da Defesa Nacional, 2015.
- NUNES, Paulo – **Sociedade em rede, ciberespaço e guerra de informação:** ***contributos para o enquadramento e construção de uma estratégia nacional de informação.*** 2.ª Ed. Lisboa: Instituto da Defesa Nacional, 2016. ISBN 978-972-9393-34-1.
- OCS – **Cyber Security Strategy of the United Kingdom - safety, security and resilience in cyber space.** Norwich: TSO, 2009.
- OLIVEIRA, Guerreiro – **Terrorismo Transnacional. Conhecer o Inimigo.** Lisboa: Instituto de Estudos Superiores Militares, 2008. Trabalho de Investigação Individual do CEMC – 2007/08.
- OLIVEIRA, Margarida – **Proteção de Dados Pessoais nas Comunicações Eletrónicas: O papel da CNPD e da ANACOM.** Lisboa: Universidade Católica Portuguesa, Faculdade de Direito, 2015. Dissertação de Mestrado.
- OTERO, Paulo – **O Poder de Substituição em Direito Administrativo: Enquadramento Dogmático-Constitucional.** Vol. I e II. Lisboa: Lex, 1995.
- PARAÍSO, Ariana – Da sociedade em rede e do novo espectro de ameaças: o ciberespaço In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 54 Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2017.
- Parecer n.º 11/2011 da Procuradoria-Geral da República. **Diário da República II Série.** N.º 109 (05-06-2012). p. 20509-20519.

- PEREIRA, André; QUADROS, Fausto de – **Manual de Direito Internacional Público.** 3ª Ed. Coimbra: Almedina, 1997.
- PEREIRA, Joana – O Ciberespaço e a Mutação da Realidade: o caso dos EUA. In **IDN Brief**. Lisboa: Instituto da Defesa Nacional, IDN Publicações, 2013. ISSN 2182-5327.
- PEREIRA, Júlio – Cibersegurança – O Papel do Sistema de Informações da República Portuguesa. In **Segurança e Defesa**. Maio-Agosto 2012. Lisboa: Diário de Bordo, 2012.
- PERES, Remi – **A guerra no Ciberespaço: princípios da guerra clássica aplicados na Ciberguerra.** Lisboa: Academia Militar, 2010. Dissertação de Mestrado.
- PIGNATELLI, Marina – **Os Conflitos Étnicos e Interculturais.** Lisboa: Instituto Superior de Ciências Sociais e Políticas, 2010.
- PINHO, Frederico – **Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados.** Porto: Faculdade de Ciências da Universidade do Porto, Departamento de Ciência de Computadores, 2017. Dissertação de Mestrado.
- PINTO, Rui – **Novas fronteiras criadas pelos ciberataques. Um novo desafio para a cooperação internacional.** Lisboa: Instituto de Estudos Superiores Militares, 2013. Trabalho de Investigação Individual do CPOG – 2012/13.
- PROCURADORIA-GERAL DA REPÚBLICA – **Gabinete Cibercrime. Relatório da Actividade.** Lisboa: Procuradoria-geral da República – Gabinete Cibercrime, 2013.
- PROCURADORIA-GERAL DA REPÚBLICA – **Jurisprudência sobre Prova Digital.** Nota Prática nº 12/2017.Lisboa: Procuradoria-geral da República – Gabinete Cibercrime, 2017.
- QUADRADO, António – **A Estratégia de Segurança Interna da União Europeia.** Lisboa: Instituto de Estudos Superiores Militares, 2015. Trabalho de Investigação Individual do CEMC – 2014/15.
- RAMALHO, David – **Métodos Ocultos de Investigação Criminal em Ambiente Digital**. Coimbra: Almedina, 2017.
- RAMOS, Armando – A novíssima diretiva relativa ao cibercrime. In SOUSA, Constança Urbano de (coord.) **O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes**. Lisboa: Ediual, 2014, p. 176-192. ISBN: 9789898191618.
- RAMOS, Armando – **A Prova Digital em Processo Penal.** Lisboa: Chiado Editora, 2014. Versão eBook.

- RAPOSO, Rogério **– O Ciberterrorismo, mecanismos de controlo e preservação da prova.** Lisboa: Gabinete Nacional de Segurança, 2013.
- RC-OP – **Regulamento de Campanha - OPERAÇÕES**. Lisboa: Estado Maior do Exército, 2005.
- Resolução do Conselho de Ministros n.º 115/2017. **Diário da República I Série.** N.º 163 (24-08-2017). p. 5035-5037.
- Resolução do Conselho de Ministros n.º 92/2019. **Diário da República I Série.** N.º 108 (05-06-2019). p. 2088-2095.
- RIBEIRO, António – **Teoria Geral da Estratégia: O Essencial ao Processo Estratégico.** Coimbra: Edições Almedina, 2009.
- RIBEIRO, Pedro – **Dados Bancários Enquanto Dados Sensíveis**. Porto: Faculdade de Direito da Universidade de Direito, 2011. Dissertação de Mestrado.
- RID, Thomas; BUCHANANA, Ben – **Attributing Cyber Attacks.** London: Journal of Strategic Studies, 2014.
- ROBINSON, et al – **Cyber-security threat characterisation.** RAND Europe, 2013.
- RODRIGUES, Benjamim – **Direito Penal Parte Especial.** Tomo I. Coimbra: Direito Penal Informático-Digital, 2009.
- RODRIGUES, Francisco – Principais ameaças no contexto da Cibersegurança. In **CEDIS Working Papers. Direito, Segurança e Democracia.** N.º 48. Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2016.
- RODRIGUES, Pedro – **Segurança informática de redes e sistemas.** Vila Real: Universidade de Trás-os-Montes e Alto Douro, 2010. Dissertação de Mestrado.
- ROHOZINSKI, Rafal – **Tracking GhostNet: Investigating a Cyber Espionage Network.**Toronto: University of Toronto, 2009.
- SANTOS, Aristofanes – **O uso da força no exercício da função policial (Alguns aspectos legais).** Lisboa: Instituto Superior de Ciências Policiais e de Segurança Interna, 2002. Tese de Licenciatura.
- SANTOS, Henrique – ***Soft Power* e *Hard Power*: dicotomia ou complementaridade.** Lisboa: Instituto de Estudos Superiores Militares, 2015. Trabalho de Investigação Individual do CPOG – 2014/15.
- SANTOS, José – **Contributos para uma melhor governação da cibersegurança em Portugal.** Lisboa: Faculdade de Direito da Universidade Nova de Lisboa, 2011. Dissertação de Mestrado.

- SANTOS, José – **As Guerras que já aí estão e as que nos esperam - se os políticos não mudarem.** Mem Martins: Publicações Europa-América, 2009.
- SANTOS, Lino; GUEDES, Armando – Breves Reflexões sobre Poder e Ciberespaço. In **Revista de Direito e Segurança.** Ano III. N.º 6. 2015. (julho/dezembro). ISSN 2182-8687.
- SANTOS, Lino et al. – Proteção do Ciberespaço: Visão Analítica. In SOARES, C.; TEIXEIRA, A.; JACINTO, C. (eds.) – **Riscos, Segurança e Sustentabilidade.** Lisboa: Edições Salamandra, 2012. ISBN 978-972-689-247-2.
- SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos – **Cyberwar – O Fenómeno, as Tecnologias e os Atores.** Lisboa: FCA, 2008.
- SANTOS, Sofia – **O uso da força no direito internacional e os desafios ao paradigma onusiano.** Belo Horizonte: Revista da Faculdade de Direito da Universidade Federal de Minas Gerais. N.º 61, Julho-Dezembro, 2012. p. 533-568.
- SANTOS, Sofia – **A Reforma dos Instrumentos Militares e da Autoridade do Conselho de Segurança das Nações Unidas na Implementação de Medidas Coercitivas Militares**. Janus.net, e-journal of International Relations, OBSERVARE. Vol. 4. N.º 1. 2013. p. 1-17.
- SANTOS, Sofia – "**O Tribunal Penal Internacional e a construção de uma ordem pública internacional**", Janus.net, e-journal of International Relations, OBSERVARE. Vol. 5. N.º 2. 2014. p. 16-45.
- SARAIVA, Rodrigo – **Legítima defesa ou represália? O uso da força no conflito armado de 2001 no Afeganistão.** São Paulo: Faculdade de Direito da Universidade de São Paulo, 2009. Dissertação de Mestrado.
- SCHMITT, Michael – International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. In **Harvard International Law Journal.** Vol. 54. Harvard: Harvard College, 2012.
- SÉNECA, Hugo – A guerra não acabou. Nem vai acabar. In **Exame Informática.** Fevereiro de 2017. p. 59-67.
- SERENO, José – **Tendências de implementação e segurança nas redes wireless organizacionais**. Setúbal: Instituto Politécnico de Setúbal. Escola Superior de Ciências Empresariais, 2015. Dissertação de Mestrado.
- SILVA, Andréia; SOARES, Cínthia; ULYSSÉA, Isabelle – **Hackers e Crackers**. Brasília: Universidade Católica de Brasília, [s. d.]. Trabalho de Pós-Graduação.

- SILVA, Nuno – **Segurança e Defesa Nacional: o desenvolvimento de capacidades de Ciberdefesa.** Lisboa: Instituto de Estudos Superiores Militares, 2012. Trabalho de Investigação Individual do CEMC – 2011/12.
- SILVA, Susana – **A Ciberespionagem no contexto Português.** Lisboa: Academia Militar, 2014. Dissertação de Mestrado.
- SILVA, Tiago – **A ameaça terrorista em Portugal.** Lisboa: Universidade Nova de Lisboa, Faculdade de Ciências Sociais e Humanas, 2015. Tese de Doutoramento.
- SIMAS, Diana – **O Cibercrime.** Lisboa: Universidade Lusófona de Humanidades e Tecnologias, 2014. Dissertação de Mestrado.
- SISTEMA DE SEGURANÇA INTERNA – **Relatório Anual de Segurança Interna de 2017.** Lisboa: Ministério da Administração Interna, 2018.
- SISTEMA DE SEGURANÇA INTERNA – **Relatório Anual de Segurança Interna de 2018.** Lisboa: Ministério da Administração Interna, 2019.
- SKOUDIS, Ed. **Counter Hack A Step by Step Guide to Computer Attacks and Effective Defenses.** PrenticeHall: Canada, 2006. Capítulo 9, Phase 3.
- SOUSA, António – **A Polícia no Estado de Direito.** Lisboa: Editora Saraiva, 2009.
- STRATEGOR – **Política Global da Empresa: Estratégia, Estrutura, Decisão, Identidade.** 3ª Ed. Lisboa: Dom Quixote, 2000. ISBN 972-20-1706-3.
- SYMANTEC – **Relatório de Ameaças à Segurança de Sites.** 2015.
- TEIXEIRA, Paulo – **O fenómeno do *Phishing*. Enquadramento jurídico-penal**. Lisboa: Universidade Autónoma de Lisboa, 2013. Dissertação de Mestrado.
- TELES, Tiago – **Cibersegurança. Deteção de outliers.** Lisboa: Escola Naval, 2015. Dissertação de Mestrado.
- THE WHITE HOUSE – **Secure Cyberspace.** GOV US Executive Branch, 2003. 2–4.
- TIKK, Eneken. **Cyber Attacks Against Georgia: Legal Lessons Identified.** Tallinn: NATO, 2008.
- TIKK, Eneken et al – **International Cyber Incidents.** Tallinn: CCDCOE, 2010.
- TIKK, Eneken – **Comprehensive legal approach to cyber security.** Estonia: University of Tartu, Faculty of Law, 2011. Tese de Doutoramento. ISBN 978-9949-19-763-7.
- TREND MICRO – Report on Cybersecurity and Critical Infrastructure in the Americas. In **Analysis and Commentary on the State of Cybersecurity in Critical Infrastructure in the Americas.** Organization of American States.

- UNIÃO EUROPEIA – **Projecto de estratégia da segurança interna da União Europeia: "Rumo a um modelo europeu de segurança".** Bruxelas: Conselho da União Europeia, 2010.
- UNIÃO EUROPEIA – **Agenda Europeia para a Segurança.** COM(2015) 185. Estrasburgo, 2015.
- UNIÃO EUROPEIA – **Visão partilhada, ação comum: uma Europa mais forte. Estratégia global para a política externa e de segurança da União Europeia.** 2016.
- VARINO, Alexandre – **Terrorismo: a interrupção de sistemas.** Lisboa: Instituto de Estudos Superiores Militares, 2012. Trabalho de Investigação Individual do CEMC – 2011/12.
- VATIS, M. – The Council of Europe Convention on Cybercrime. In: **National Research Council of The National Academies, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.** Washington D.C.: The National Academies Press, 2010. p. 207-223.
- VAZ, Ana – Segurança da Informação, Proteção da Privacidade e dos Dados Pessoais. In **Nação e Defesa.** N.º 117. 3.ª Série. Lisboa: Instituto de Defesa Nacional, 2007. p. 35-63.
- VELOSO, Ana Flávia. Ação relativa a ameaças à paz, ruptura da paz e atos de agressão: art.º 51. In BRANT, Leonardo (Org.). **Comentário à Carta das Nações Unidas.** Belo Horizonte: Centro de Direito Internacional, 2008.
- VERDELHO, Pedro – A obtenção da prova no ambiente digital. In **Revista do Ministério Público.** N.º 99. Ano 25. Julho-Setembro 2004.
- VERDELHO, Pedro – **A nova Lei do Cibercrime.** Scientia Juridica, 2009. 320(58).
- VIEIRA, Rui – **A Prova Digital.** Lisboa, Universidade Autónoma de Lisboa, 2015. Pós-graduação em Ciências Criminais.
- VIHUL, Michael – The Nature of International Law Cyber Norms. In OSULA, Anna-Maria; RÕIGAS, Henry. **International Cyber Norms. Legal, Policy & Industry Perspectives.** Tallinn: CCDCOE, 2016. ISBN 978-9949-9544-7-6. p. 34-35.
- VILELA, Carolina – **A Gestão de Crises no Quadro da NATO.** Lisboa: Universidade de Lisboa, Instituto Superior de Ciências Sociais e Políticas, 2013. Dissertação de Mestrado.
- WAMALA, F. – **The ITU National Cybersecurity strategy guide.** International Telecommunication Union, 2011.

- WARREN, M. – **Terrorism and the Internet. Cyber Warfare and Cyber Terrorism.** Information Science Reference, 2008. p. 129–153.
- WEBER, M. – **Ciência e Política duas vocações**. 14º Ed. Berlim: Dunker & Hunblot, 2007.
- WEIMANN, G. – **New Terrorism and New Media.** Wilson Center Common Labs, 2014.
- WU, H.; ZHAO, L. **Web Security: A WhiteHat Perspective.** Chapter 13: Application-Layer Denial-of-Service Attacks. 2015.

Sítios na Internet:

- AAVV – **Critical Infrastructure Protection: Threats, Attacks and Countermeasures.** Roma: Tenace Editora, 2014 [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf.
- ALEXANDER, Keith– **United States Strategic Command.**2010. [Em Linha]. [Consult. 25 Jun. 2018]. Disponível em WWW:<URL: http://www.stratcom.mil/factsheets/cc/.
- BALDONI, Roberto – Critical Infrastructure: Definitions and Concepts. In **Protecting National Critical Infrastructures from Cyber Threats.** Rome: TENACE Project, 2014. [Consult. 15 Mar. 2018]. Disponível em WWW:<URL: http://www.dis.uniroma1.it/~tenace/.
- BARRETO, Renata – **A guerra como meio de solucionar conflitos internacionais.** [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_art.ºs_leitura&art.º_id=1679.
- BOUVIER, Antoine – **Direito Internacional Humanitário e Direito dos Conflitos Armados.** [Em Linha]. Williamsburg: Instituto para Treinamento em Operações de Paz, 2018. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://cdn.peaceopstraining.org/course_promos/international_humanitarian_law/international_humanitarian_law_portuguese.pdf.
- BOTEK, Adam – **Regime Sancionatório da UE para ataques cibernéticos.** Agência Nacional de Segurança da Informação e Cibernética da República Checa. CCDCOE – INCYDER. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/.

- BRANCO, Margarida – **A importância da criação da base de dados Passenger Name Record (PNR) como meio de investigação criminal na União Europeia.** [Em Linha].Lisboa: Universidade Autónoma de Lisboa, 2017. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: http://hdl.handle.net/11144/3010.
- BRANDES, Sean – **The Newest Warfighting Domain: Cyberspace.** [Em Linha]. 2013. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.synesisjournal.com/vol4_g/Brandes_2013_G90-95.pdf.
- BRAVO, Rogério – **Dos vestígios em ambiente digital à prova digital como intelligence.** [Em Linha]. 2009. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.academia.edu/4691991/DOS_VEST%C3%8DGIOS_EM_AMBIENTE_DIGITAL_%C3%80_PROVA_DIGITAL_COMO_INTELLIGENCE.
- CASTELLS, Manuel – **A Sociedade em Rede. A Era da Informação: Economia, Sociedade e Cultura.** [Em Linha]. Vol. I. Fundação Calouste Gulbenkian CERT-EU. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://cert.europa.eu/cert/plainedition/en/cert_about.html.
- CAVELTY, M. – **A Resilient Europe for an Open, Safe and Secure Cyberspace.**UI Ocasional Papers 23, 2013. [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.ui.se/globalassets/ui.se-eng/publications/ui-publications/a-resilient-europe-for-an-open-safe-and-secure-cyberspace-ilovepdf-compressed.pdf. p. 3-13.
- CHRISTOU, G. – **The EU's Approach to Cyber Security.** Colchester: University of Essex, 2017. [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://repository.essex.ac.uk/19872/1/EU-Japan_9_Cyber_Security_Christou_EU.pdf.
- COMITÉ INTERNACIONAL DA CRUZ VERMELHA – **O DIH e outros regimes legais – jus ad bellum e jus in bello.** [Consult. 12 Out. 2018]. Disponível em WWW:<URL: https://www.icrc.org/por/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm.
- COMPUTERWORLD – **Previsões de cibersegurança para 2018.** [Em Linha]. [Consult. 25 Jun. 2018]. Disponível em WWW:<URL: https://www.computerworld.com.pt/2017/12/22/previsoes-de-ciberseguranca-para-2018/#.Wj6cKwdJdmM.email.
- CONSELHO DA UNIÃO EUROPEIA – **Cibersegurança na Europa: regras mais rigorosas e uma melhor proteção.** [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://www.consilium.europa.eu/pt/policies/cyber-security/.

- CONSELHO DA UNIÃO EUROPEIA – **Conselho aprova regras em matéria de cibersegurança a nível da UE.** [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL:http://www.consilium.europa.eu/pt/press/pressreleases/2016/05/17widecybersecurityruleadopted/.
- COPETO, Rogério – **Cibercriminalidade.** [Em Linha].[Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://www.lidadornoticias.pt/opiniao-rogerio-copeto-oficial-da-gnr-cibercriminalidade/.
- COSTA, João – **Cibercriminalidade. Enquadramento jurídico nacional e europeu** [Em Linha]. Lisboa: Universidade Nova de Lisboa, Faculdade de Direito, 2012. IX Curso de Mestrado em Direito e Segurança. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL:http://www.academia.edu/10077810/CIBERCRIMINALIDADE_ENQUADRAMEN-TO_JUR%C3%8DDICO_NACIONAL_E_EUROPEU_Cibercriminalidade_Enquadramento_Jur%C3%ADdico_Nacional_e_Europeu-_IX_CURSO_DE_MESTRADO_EM_DIREITO_E_SEGURAN%C3%87A.
- **Dicionário Diplomático**. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://dicionariodiplomatico.blogspot.pt/2003/11/j.html.
- DISRF – **Doctrine of the Information Security of the Russian Federation.** 2000. [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.medialaw.ru/e_pages/laws/project/d2-4.htm.
- DONEDA, Danilo – **Um Código para a proteção de dados pessoais na Itália.** [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.researchgate.net/profile/Danilo_Doneda/publication/266036287_Um_Codigo_para_a_protecao_de_dados_pessoais_na_Italia/links/5934046b0f7e9beee7bcd261/Um-Codigo-para-a-protecao-de-dados-pessoais-na-Italia.pdf.
- ENISA – **Electronic evidence – a basic guide for First Responders. Good practice material for CERT first responders.** United Kingdom: Northumbria University, 2014. ISBN 978-92-9204-111-3. [Consult. 27 Mar. 2019]. Disponível em WWW:<URL: https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders.
- EUROPEAN COMMISSION – **Cybersecurity. Digital Agenda for Europe.** [Em Linha] [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://ec.europa.eu/digital-agenda/en/cybersecurity.

- GUARDA NACIONAL REPUBLICANA – **Estratégia da Guarda 2020 – Uma Estratégia de Futuro**. [Em Linha].[Consult. 03 Jan. 2018]. Disponível em WWW:<URL:http://www.gnr.pt/portal/internet/dcrp/EG2020/eg2020.swf.
- INSTITUTO DE CIÊNCIAS JURÍDICO-POLÍTICAS – **Direito da Cibersegurança e do Ciberespaço.** [Em Linha]. Lisboa: Faculdade de Direito da Universidade de Lisboa, 2018. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.icjp.pt/cursos/14278/programa?language=en.
- JENIK, A. – **Cyberwar in Estonia and the Middle East.**Network Security, 2009.N.º 4. [Em Linha]. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: https://doi.org/10.1016/S1353-4858(09)70037-6. p. 4-6.
- JP 1-02. – **Department of Defense Dictionary of Military and Associated Terms.** 2009.
- JP 2-01.3. – **Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace.** 2000.
- KRUPCZYNSKI, M. – **NATO's Reaffirmed Commitment to Cyber Security.** 2016. [Em Linha]. [Consult. 15 Out. 2018]. Disponível em WWW:<URL: http://futurenato.org/articles/natos-reaffirmed-commitment-to-cyber-security/.
- LEITÃO, Luís Meneses – **A Responsabilidade Civil na Internet.** [Em Linha]. Conferência realizada na Associação Empresarial de Portugal, em 16 de novembro de 2000. [Consult. 21 Set. 2018]. Disponível em WWW:<URL: http://www.oa.pt/upl/%7B034a6b68-6f5e-4eb9-b57b-06a413387077%7D.pdf.
- LESK, M. – **The new front line: Estonia under cyberassault.** IEEE Security & Privacy, 2007. 5(4). [Em Linha].[Consult. 27 Mar. 2017]. Disponível em WWW:<URL: //dx.doi.org/10.1109/MSP.2007.98. p. 76-79.
- LIIK, K. – **The "Bronze Year" of Estonia-Russia relations.** Tallinn: Ministry of Foreign Affairs of Estonia, 2007. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: http://vm.ee/sites/default/files/content-editors/web-static/053/ Kadri_Liik.pdf.
- **Manual de Tallinn: A Segurança Cibernética.** [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://agnfilho.webnode.com/news/manual-de-talinn%3A-a-seguran%C3%A7a-cibernetica-/.
- MEULEN, N.; JO, E.; SOESANTO, S. – **Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.** Justice, Freedom and Security,

2015. [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://dx.doi.org/10.7249/RR1354. p. 1-152.

- NATÁRIO, Rui – **O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço.** [Em Linha]. Lisboa: Revista Militar, 2016. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.revistamilitar.pt/artigo.php?art_id=854.
- NATO – **Cyberdefence.** 2016. [Em Linha]. [Consult. 15 Out. 2018]. Disponível em WWW:<URL: https://www.nato.int/cps/en/natohq/topics_78170.htm.
- NICKOLOV, Eugene – **Critical information infrastructure protection: analysis, evaluation and expectations.** [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.comw.org/tct/fulltext/05nickolov.pdf.
- NUNES, Flávio – **Cibersegurança. "Estamos em guerra, meus senhores".** [Em Linha]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://observador.pt/2016/04/13/cibersegurancaestamosguerrameussenhores/.
- NUNES, Paulo – Ciberterrorismo: Aspectos de Segurança. In **Revista Militar.** N.º 2433. Outubro de 2004. [Consult. 15 Mar. 2018]. Disponível em WWW:<URL: https://www.revistamilitar.pt/artigopdf/4282.
- NUNES, Paulo – **Mundos virtuais, riscos reais: fundamentos para a definição de uma estratégia da informação nacional.** [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://icnsd.afceaportugal.pt/conteudo/congresso/ICNSD_4G_texto_pdf_paulo_viegas_nunes.pdf.
- PALMA, Fernando – **Gerenciamento de Incidentes de Segurança da Informação passo a passo.** 2014. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: https://www.portalgsti.com.br/2014/01/gerenciamento-de-incidentes-de-seguranca-da-informacao-passo-a-passo.html.
- **Portal de Cibersegurança da GNR** [Em Linha]. [Consult. 05 Out. 2019]. Disponível em WWW:<URL: http://portalciber.gnr.local/wordpress/index.php/2015/12/28/seguranca-na-internet/.
- RAMMINGER, Erica. **O conceito de auto-defesa na Carta da ONU e a Guerra no Iraque: Guerra preventiva ou preemptiva?**[Em Linha]. [Consult. 05 Out. 2019]. Disponível em WWW:<URL: www.cedin.com.br/revistaeletronica/art.ºs.

- ROBERT, Petit – **Le nouveau Petit Robert de la Langue Française 2010.**[Em Linha]. [Consult. 05 Mai. 2019]. Disponível em WWW:<URL: http://pr2010.bvdep.com/version-1/pr1.asp.
- ROSA, Patrícia; SILVA, Carla – **O uso da força em direito internacional – legítima defesa preemptiva.** Universidade de Itaúna, [s.d.]. [Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.publicadireito.com.br/artigos/?cod=a08c938c1e7c76d8.
- SANTOS, Diana; SILVA, Rita – **Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001** [Em Linha]. Porto: Universidade do Porto, Faculdade de Engenharia, 2012. Trabalho de Segurança de Informação do MCI 2012/2013. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: https://web.fe.up.pt/~jmcruz/seginf/seginf.1314/trabs-als/final/G4-ISO.27000.final.pdf.
- SANTOS, Paulo – **Furto de Identidade *On-line*.** [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://portalciber.gnr.local/wordpress/index.php/2015/12/21/furto-de-identidade-on-line/.
- SCHJOLBERG, S. – **Computer-related offences.** Conselho da Europa, 2004. [Consult. 10 Out. 2018]. Disponível em WWW:<URL: http://cybercrimelaw.net/documents/Strasbourg.pdf.
- TVNET – **A guerra no ciberespaço.** 2009. [Em Linha]. [Consult. 27 Mar. 2018]. Disponível em WWW:<URL: http://tvnet.sapo.pt/noticias/video_detalhes.php?id=44111.
- **U. S. Cyber Command.** 2016. [Em Linha].[Consult. 03 Jan. 2018]. Disponível em WWW:<URL: www.cybercom.mil/About/History/.
- VEIGA, Pedro; DIAS, Marta – **A Internet e as novas dimensões legais.** [Em Linha]. Lisboa: Universidade Autónoma de Lisboa, 2012. [Consult. 27 Mar. 2017]. Disponível em WWW:<URL: http://janusonline.pt/popups2011_2012/2011_2012_1_5.pdf.
- WIRED – **Hackers Take Down the Most Wired Country in Europe.**[Consult. 30 Jun. 2016]. Disponível em WWW:<URL: http://www.wired.com/2007/08/ff-estonia.
- WORLD ECONOMIC FORUM –**The Global Risks Report 2015.**[Consult. 12 Out. 2018]. Disponível em WWW:<URL: http://www.weforum.org/reports/global-risks-report-2015.
- YAPP, P. – **The National Cyber Security Centre Incident Management.** London: National Cibersecurity Centre, [s.d.]. [Em Linha].[Consult. 03 Jan. 2018]. Disponível em WWW:<URL: www.owasp.org/images/1/1e/NCSC_slides.pdf.